Naval Research Laboratory
Washington, DC 20375-5320

NRL/MR/5529--95-7770

Digital Telephony Analysis Model and Issues

LYNN M. KEUTHAN

Communication Systems Branch
Information Technology Division

September 1, 1995

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1, 1995	Final 3/93-8/93

4. TITLE AND SUBTITLE

Digital Telephony Analysis Model and Issues

5. FUNDING NUMBERS

PE-0603013N/F1947

6. AUTHOR(S)

Lynn M. Keuthan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5529--95-7770

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
800 North Quincy Street
Arlington, VA 22217-5660

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

Experts in the fields of digital telephony and communications security have stated the need for an analytical tool for evaluating complex issues. Some important policy issues discussed by experts recently include implementing digital wire-taps, implementation of the "Clipper Chip", required registration of encryption/decryption keys, and export control of cryptographic equipment. Associated with the implementation of these policies are direct costs resulting from implementation, indirect cost benefits from implementation, and indirect costs resulting from the risks of implementation or factors reducing cost benefits. Presented herein is a model for analyzing digital telephony policies and systems and their associated direct costs, and indirect benefit and risk factors. In order to present the structure of the model, issues of national importance and business-related issues are discussed. The various factors impacting the implementation of the associated communications systems and communications security are summarized, and various implementation tradeoffs are compared based on economic benefits/impact. The importance of the issues addressed herein, as well as other digital telephony issues, has greatly increased with the enormous increases in communication system connectivity due to the advance of the National Information Infrastructure.

14. SUBJECT TERMS

Digital telephony
Digital telephony security
Wiretap implementation
Clipper chip
Registration of encryption/decryption keys
Export control of cryptography

15. NUMBER OF PAGES

109

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18
298-102

Table Of Contents:

Tables:

Figures:

DIGITAL TELEPHONY ANALYSIS MODEL AND ISSUES

1.0 Executive Summary

Experts in the fields of digital telephony and communications security have stated the need for an analytical tool for evaluating complex issues [13]. Some important policy issues discussed by experts recently include implementing digital wire-taps, implementation of the 'Clipper Chip', required registration of encryption/decryption keys, and export control of cryptographic equipment. Associated with the implementation of these policies are direct costs resulting from implementation, indirect cost benefits from implementation, and indirect costs resulting from the risks of implementation or factors reducing cost benefits. Presented herein is a model for analyzing digital telephony policies and systems and their associated direct costs, and indirect benefit and risk factors. In order to present the structure of the model, issues of national importance and business-related issues are discussed. The various factors impacting the implementation of the associated communications systems and communications security are summarized, and various implementation tradeoffs are compared based on economic benefits/impact. The importance of the issues addressed herein, as well as other digital telephony issues, has greatly increased with the enormous increases in communication system connectivity due to the advance of the National Information Infrastructure. Debates over communication legislation such as the implementation of wire-taps, 'Clipper Chip' implementation, registration of encryption/decryption keys, and export control of cryptographic technology have resulted from the creation of 'information super highways' that interconnect agencies, businesses, and individuals.

The increasing demand for communication services has been highlighted several times by the media [29,39]. The New York Times recently stated "Internet is currently the world's most fashionable rendezvous. It touches down in 137 countries and links 15 million to 30 million people and is growing by a million users each month." [39] Technical issues of importance to those implementing secure LANs and to those developing policy and technology for the National Information Infrastructure are used to demonstrate the broad usefulness of the model. Several political and business-related issues arise from this increase in telecommunications. One common business-security concern is data

Manuscript approved March 23, 1995.

confidentiality, resulting in the need for securing communications between a company's various locations, for instance, between field offices and headquarters. Once the need for secure communications has been established, a business must decide how to obtain secure communications and to what extent (or what methods of) communication must be secure. For instance, are voice communications the only concern? Are important transactions handled by computers? If so, is security of the computer communications across a wide area network (WAN) a concern? There have been some discussions recently regarding the need for secure FAX communications [17,44]. If secure voice, data, or FAX transmission is required, how many lines need to be secured? Will one secure line meet the requirements for secure communication of proprietary information, or should all lines be secured to prevent inadvertent disclosures over a non-secure line? If a business has decided to install secure communications at some point in time, should a secure system be purchased up front and financed, or can security be added later with minimal impact (when more funds are available)? Once the need for secure communications has been established to protect company information, trade secrets, non-disclosure agreements, and/or individual/personal information, what types of secure communications are available and how do they compare in cost? Encryption of information is becoming a common means by which an organization provides data confidentiality and non-disclosure. One primary tradeoff with regard to encryption of data is hardware encryption vs. software encryption. Other tradeoffs revolve around types of physical level security devices and the differences in products and costs between vendors/manufacturers. Two scenarios are developed to demonstrate the use of the model in analyzing these primary business concerns, One: Security Implementation Tradeoffs, and Two: Initial Installation vs. Retrofit of Security Capabilities.

Common issues of interest on a national scale were obtained from the media, pertinent Internet news groups (such as the Forum On Risks To The Public In Computers And Related Systems, the ACM Committee on Computers and Public Policy, moderated by Peter G. Neumann [28]), laws pertaining to the use of communication security equipment [34], and published statistics regarding the usage of communication equipment [5,49,51] and the cost of crime [4,8,23,24,33,38,45,54,56]. Within the last two years, two national intelligence agencies have developed legislative proposals that have met with a great deal of opposition (the 'Digital Telephony Proposal' presented by the Federal Bureau of Investigation (FBI) and the 'Clipper Chip' proposal presented by the National Security Agency (NSA)). The 'Digital Telephony Proposal' submitted by the FBI would require telephone communication providers to

build wire tap features into new communication hardware [25]. The FBI had previously obtained the support of AT&T for the 'Digital Telephony' proposal, and AT&T had agreed to redesign broadband communication equipment to support the wire tap capability if the proposal passed [10]. Corporate leaders of other telephone providers had also provided support privately, but withdrew support once their engineers became aware of the proposal and explained the enormous cost that would be incurred and the loss of networking capability [10]. Once the content of the 'Digital Telephony' proposal became generally known, it suffered a great deal of opposition and was defeated on the House floor [3]. The primary reason cited for opposition was the enormous cost of redesigning broadband equipment. A separate scenario, Scenario Three, was developed to examine the implementation of the wire-tap capability and the Digital Telephony model was used to compare the cost of implementation of the wire-tap capability vs. the cost of not implementing the wire-tap capability. The comparisons were based on several parameters, including the cost of wire-tapping and the cost of crime. The scenario development and analysis of the wire-tapping issue takes into account the analysis provided by some of the industry experts [20,26].

A recent initiative on the part of the National Security Agency was to mandate the use of a key escrow system and use of a specific encryption device, the 'Clipper Chip', in all public communications [6]. This proposed mandate on the use of the 'Clipper Chip' was also met with a great deal of opposition, especially from U.S. hardware and software encryption manufacturers [37], and from organizations promoting individual rights, such as the American Civil Liberties Union (ACLU) [2,26,47,58]. U.S. hardware and software encryption manufacturers have invested resources in the research, design, and development of encryption devices and software, and naturally do not want their market in these products to be erased. Many of these manufacturers believe that even voluntary use of a federally supported encryption device will severely affect the available market of their products and, therefore, oppose the Government's efforts to make the chip generally available. Since the encryption algorithm used in the 'Clipper Chip' (the SKIPJACK Algorithm) has not been made available in its entirety, these manufacturers have questioned its strength, resulting in a review and analysis of the algorithm by a selected number of industry experts that verified the algorithm's strength [9]. Other industry experts have attacked any regulation of cryptography as a deterrence to advancements proposed by the Information Infrastructure Task Force [37]. James Kobielus states "Commercial development of the promised Information Superhighway depends on the availability of cheap, efficient, powerful crypto technologies." [37] Organizations promoting

individual rights have also voiced concerns that the Government's mandate of a standard puts too much power in the hands of the Government and that abuse of that power by the Government is likely [2]. These organizations also believe that promotion of a standard on a voluntary basis would still give the Government too much power, since the Government's promotion of the single device would make it the only viable encryption solution with regard to cost and availability for most individuals and businesses [14]. Since several groups have lobbied against this initiative, it is unlikely at this point that use of the 'Clipper Chip' will be mandated. It is much more probable that the 'Clipper Chip' will be used on a voluntary basis by the commercial sector [42]. The 'Clipper Chip' is, however, slated for use by the Government for all non-classified communications [6,9,42]. Therefore, the current trend for use of the 'Clipper Chip' is large scale use in Government and commercial communications with other forms of encryption used on a smaller scale. Scenario Four addresses the issues around the 'Clipper Chip' and the costs of implementation to the Government, individuals, and telephone companies, and the cost in possible lost revenues for hardware and software encryption companies. Also included is the cost of crime as might be affected by the Government's inability to decipher communications in a timely manner during investigations because of the use of other encryption products.

Two related issues are the registration of encryption/decryption keys, which are addressed in Scenario Five, and export controls on cryptographic technology, which is addressed in Scenario Six. The FBI proposed requiring the registration of all keys used for encryption and decryption of communications in their 'Digital Telephony' proposal [25]. Registration of keys would allow the law enforcement agencies to obtain warrants to obtain registered keys, when authorized, for investigations. Individuals with improperly registered keys would be fined. Of course, the question arises, why would those intending to perpetrate organized crime bother to properly register their keys? A much less severe penalty might result from improperly registered keys than that from a conviction connected to organized crime. Clearly, the benefit of requiring properly registered keys would be directly related to the percentage of keys properly registered in cases where a warrant had been obtained. For example, if all keys had been properly registered for all cases in which warrants had been obtained, then this proposal would be clearly beneficial for law enforcement agencies. On the other hand, if no keys had been properly registered for the cases in which warrants had been obtained, then the cost of such a proposal would surely outweigh any benefit obtained by imposing fines for improperly registered keys. Obviously, the costs, risks, and benefits of such a proposal are quite complex with many

interdependent factors. Scenario Five addresses a probabilistic scenario given the proposed legislation without additional modification. (Lawmakers could find innumerous variations on methods of implementing such a proposal.)

U.S. export controls on cryptographic devices have been in effect since the '70's when the RSA (Rivest, Shamir, and Adelman) algorithm was first restricted from export [34,46,57,59]. Since the export restrictions were initiated, several variations of the RSA algorithm have been made available over the Internet [33], yet the export restrictions remain in effect to provide some impediment to criminals obtaining the algorithm [43]. Unfortunately, similar restrictions do not exist for foreign companies who might want to market products employing the algorithm, creating an inequitable balance of opportunities in cryptographic devices that favors foreign companies [13]. U.S. companies, such as Hewlett-Packard, Racal-Guardata, and Fisher International, have testified before the Computer System Security and Privacy Advisory Board to try to get the export restrictions lifted [27]. National security agencies seem determined, however, to keep the export restrictions in place [30]. Classified reasons for maintaining export restrictions on strong encryption algorithms might exist. Even if so, tradeoffs between the costs, risks, and benefits of continuing the current policy on exports restrictions should be evaluated in some meaningful way. Scenario Six was developed to analyze this issue, taking into account several important factors pertinent to national security and to U.S. economic interests.

The specific policy and technical issues addressed herein include: (1) security implementation tradeoffs, (2) initial design with security vs. retrofit, (3) telephone wire-tap capability implementation, (4) 'Clipper Chip' implementation, (5) registration of keys, and (6) export control of cryptographic technology. A scenario was developed surrounding each of these issues to demonstrate the application of the model for use in analyzing the tradeoffs for a specific issue. The 'information super highways' will allow the transfer of enormous amounts of data to the extent of supporting integrated real-time services including voice, audio, and video imagery [55]. As agencies, businesses, and individuals are interconnected, communication system implementation options abound, and the policies surrounding the use of communication systems and networks must be further developed and refined.

2.0 Scope

This document is intended for those who need to analyze complex digital telephony issues. Technical issues and policies may range from private business communication concerns to establishing communication policies and security procedures at an organizational or national level. At the national level several different groups are currently involved in defining and establishing policies and procedures for use of communication systems and networks. In order to aid those seeking to analyze national issues, some issues of national interest have been summarized and references for obtaining detailed information have been provided. Since models for analyzing these issues have not been readily available, an example model is presented herein for analyzing such issues based on a widely used software package, Microsoft Excel. To demonstrate the structure of the model, important factors for several issues have been compiled in database format and provide a basis for evaluation of these issues. Scenarios are used to demonstrate the exercising of the model for specific parameter values, and provide a basis for further analysis of specific issues.

3.0 Approach

General research was conducted on current issues, including political and business-related issues. Information regarding issues of interest was obtained from the media [11,14,30,39,41,42,49,53], pertinent Internet user groups (such as the "Computer Risks" user group) [28], laws pertaining to the use of communication equipment [6,9,13,16,18,22,25], published statistics regarding usage of communication equipment and the cost of crime [4,5,8,22,23,24,31,33,38,45,49,51,54,56], and magazines regarding common business security concerns [5,11,20,21,29,36,37,41,46, 50,59].

Different aspects of each issue were investigated and lists of parameters effecting each issue were developed. Realistic values for parameters were obtained from general research from sources listed above and estimates were used in other cases in order to exercise the model and demonstrate its operation. When actual values were unknown, a value of zero was entered; these cases are easily identified within the database. It is anticipated that experts in a particular area could simply fill in appropriate values and, therefore, exercise the model in a particular scenario. Provided herein is a database of hundreds of

parameters encompassing most of the important aspects of digital telephony issues, a structure within which to store and compute tradeoffs in costs, and an automated tabulation and comparison of costs associated with a technical or policy issue.

For this compendium of issues, tradeoffs, and parameters, a suitable model was constructed to analyze the costs, risks, and benefits of each possible implementation given a specific scenario. Scenarios are used to define specific tradeoffs and realistic values for a given issue. For issues commonly encountered in business, scenarios define particular business communication needs and security requirements in order to execute specific instances of the model. For national security issues, scenarios are defined based on the tradeoffs defined by the agencies, industries, organizations, and individuals debating the issue. In the construction of this model emphasis was placed on modularity and applicability to a wide range of issues important in the area of digital telephony to allow expansion of the model to account for additional parameters and to address additional issues.

In order to provide a model based on a widely-used, low-cost analytical tool, the telephony model was constructed using Microsoft Excel spreadsheets and macros. Some specific features and capabilities of Microsoft Excel made it particularly suitable for model development. Specific operations on spreadsheet values can be computed using Microsoft Excel macros and the results stored back to the spreadsheet. Microsoft Excel offers the capability to program specific operations on data within a spreadsheet[40]. Because Microsoft Excel offers this capability, it is not as 'user-friendly' as many standard database programs, but, on the other hand, is more flexible than many standard databases. Some operations also execute more quickly than on standard databases. For instance, since parameters are stored in a spreadsheet, the database program does not need to keep track of several levels of hierarchy; levels of hierarchy can be defined by format within the database. Also, values can be entered faster within the database than by entering parameters one-by-one using menus or "tabbed" entries. In addition, values utilized can be easily checked, their affect on other database values can be easily checked, and model results can be correlated with parameter values.

Within the spreadsheet a 'Digital Telephony Database' is defined. The first level in the Digital Telephony Database is comprised of the defined digital telephony issues. For each issue parameters are categorized first as (1) a direct cost, (2) indirect risk factor, or (3) an indirect benefit, and

then categorized within a group of related factors. Additional issues, categories, parameters, and values can be added within the defined structure of the database. In the definition of new issues, several existing parameters can be utilized and copied to a new section of the database. Certain parameters are also defined in the spreadsheet that are used by the macros. Values for key parameters are defined in a 'run-time' box so that they can be updated for each execution of the model. Two run-time boxes can be exercised - one that compares the costs, risks, and/or benefits for each side of an issue and displays the total cost for each, and one that displays these costs as a function of a varying parameter. These run-time parameters are:

Digital Telephony Model:
- Issue Number
- Number of Sides

Parametric Tabulation:
- Issue Number
- Side Number

Issues within the database are assigned an issue number; each parameter associated with that issue is identified by the issue number. Each issue has tradeoffs to be compared. Each possible tradeoff represents sides of the issue. For instance, in Scenario Four, dealing with the implementation of the 'Clipper Chip', a basic tradeoff exists between mandatory use of the 'Clipper Chip' and no implementation of the 'Clipper Chip'. These two sides of the issue are labeled as Side 1 and Side 2, respectively, in the database. A third possible, and very likely, tradeoff is the voluntary use of the 'Clipper Chip' for private communications. This possibility is labeled as Side 3 for Issue One ('Clipper Chip' implementation). In this case the 'Clipper Chip' would be only one possible means of securing private communications, although with the current support of the Government, the 'Clipper Chip' will probably become the most common means of securing private communications. The benefit (to national and law enforcement agencies) of implementing the 'Clipper Chip' based on voluntary use depends on the percent of individuals/organizations using the 'Clipper Chip' (and no other form of encryption) in cases where a warrant is obtained. Obviously, this percentage is an unknown parameter. Therefore, in examining the tradeoffs for the 'Clipper Chip' implementation, a parametric analysis was perform by varying this percentage from 0% to 100%. When exercising the model for the 'Clipper Chip' implementation for this tradeoff, the above parameters for the Digital Telephony Model would be set as follows:

Digital Telephony Model:
Issue Number: 1
Number of Sides: 3

An output area is also defined for writing the tabular results to the database. This defined output area is accessed by a macro routine designed to display the results of parametric analyses.

In order to search for items in a database, Microsoft Excel macros use 'search templates' contained in the spreadsheet [40]. The search template contains headings that match the headings of the columns in the 'Digital Telephony' database. A particular item within the database can be found using macros by searching for the entry in the database that matches the values given under the headings of the search criterion. Excel macros can only retrieve one entry using a search criterion. Therefore, each entry searched for must be unique and each parameter line within the database is sequentially numbered. Since Microsoft Excel macros require a defined search pattern, this sequence number is required in order to 'step' through the database. The sequence number is incremented for the search criterion as the macro iterative adds additional parametric values.

A set of macros (Telephony Cost Tabulation routine) allows the cost to be tabulated for each side of an issue. The macros use the search criterion to find all parameters that affect a particular side of an issue and maintain a running total of the costs. The economic benefits for an issue are optionally subtracted from the costs (lowering the actual cost because of financial benefits). The risks associated with an issue are optionally added to the costs (increasing the costs associated with an implementation). These options allow the model to be exercised in several ways, tabulating (1) direct costs only, (2) costs - benefits, or (3) costs + risks - benefits.

A second set of macro commands (Parametric Tabulation routine) allows the costs to be tabulated as a single parameter is varied. The macro searches the database to find the relevant issue and then find the parameter within that issue marked for parametric analysis. The macro initializes the parameter value to a starting value stored in the database, and tabulates the total costs for each side of an issue by calling the cost macro. The parametric value is then incremented by the step value, and the macro calls the cost macro again to tabulate the new total costs for each side of the issue. The macro continues incrementing the parameter value and tabulating the new total costs until the final parametric value

is reached. As calculations are made, the values of the parameter vs. tabulated total costs are stored in the database for reference and for access by the plotting routine. The Parametric Tabulation routine writes the nominal parameter value back to the 'Digital Telephony' database after costs are tabulated.

A plotting routine (Plot Parametric Values) was developed to automatically display the results of the parametric analysis. The results are displayed on an X-Y plot. 'X' and 'Y' axes and the plot title are generically labeled and the user can accept these labels as a default or enter new labels. The resulting plot can be saved to a file. Additional parametric analyses can be performed with the results of each saved to a separate file. Since the tabular results are written to the same output area within the database for various runs, these results must be copied to different places within the database (or to separate files) in order to save the tabular results.

Scenarios are used to define specific tradeoffs and realistic values for a given issue. Realistic scenarios were developed based on probabilistic factors and current trends/tradeoffs. For instance, the current trend for use of the 'Clipper Chip' is large scale use in Government and commercial communications with other forms of encryption used on a smaller scale. Given a particular issue, such as one involving the use of the 'Clipper Chip', possible tradeoffs are defined and contributing factors for each side of a tradeoff identified. The economic risks and benefits of implementing each side of the issue was computed based on identified contributing factors. For the 'Clipper Chip' example (used in Scenario Four) economic benefit was defined in regard to overall national economic benefit, including such parameters as the cost of crime, the cost of law enforcement and investigations, the cost of divulgence of proprietary business information, and the cost of divulgence of sensitive financial and medical information. Relevant parameters were identified in each case.

4.0 Trade-Offs

Several important tradeoffs were identified for the issues analyzed and identified above. Issues and tradeoffs concerning communication policy, technology, and implementation were investigated with regard to financial costs, risks, and benefits. In Scenario One, Security Implementation Tradeoffs, common tradeoffs involve software vs. hardware solutions, physical level security vs. applications level security, and tradeoffs in encryption devices and algorithms.

Scenario Two (Initial Installation vs. Retrofit of Security Capabilities) employs the use of the 'Digital Telephony Model' to examine typical tradeoffs in cost between initial installations and retrofits. A common business concern is the cost of installing security capabilities for communication. When starting up a business, costs can be rather significant, and without an established customer base, financial tradeoffs usually must be considered. Since secure communication is becoming a greater concern for many businesses, the cost of installing secure communication at the outset is a consideration for more and more businesses. The most typical tradeoff is usually higher initial cost with a lower overall cost vs. lower initial cost with higher overall cost because of retrofitting equipment. Parametric analysis can be used to calculate costs based on the percentage of transmitter/receiver pairs modified. This can be used to determine of the percentage of transmitter/receiver pairs that could be retrofitted for secure communications for the same cost as initially installing secure communication for all transmitter/receiver pairs. If all transmitter/receiver pairs will eventually be secured, the additional cost for adding security later can be factored against the cost of financing the initial installation.

In Scenario Three (Legislating Communication Equipment Wire-tap Capability), the tradeoff exists between implementing the tap capability vs. no redesign of broadband communication equipment for a tapping capability. The cost of implementation of the tap capability must be weighed against the benefits derived by national security and law enforcement agencies. Similar tradeoffs also exist for Scenario Four ('Clipper Chip' Implementation) and Scenario Six (Export Controls on Cryptography). The wire-tapping issue is somewhat more complicated because of the complexity of the technical/engineering design issues and tradeoffs. For instance, a lower cost, perfectly viable alternative to implementation of the tap capability might exist based on another engineering/technology solution. Suppose, for example, that network management protocols could be designed to store and/or retrieve particular information transferred over the network. This would entail software development that might be more economically feasible than developing a hardware wire-tapping capability.

In Scenario Four, dealing with the 'Clipper Chip', tradeoffs revolve around implementation vs. no implementation vs. limited implementation, as described in Paragraph 2.0 above. Considerations for these tradeoffs include the cost of implementation, the benefit derived by national security agencies and law enforcement agencies, and the risk of improper

use of key and/or private communication information. The cost of implementation could be broken down to consider the cost to the Government (for design and for implementation for Government use), to telephone companies, and to subscribers.

In Scenario Five (Registration of Encryption/Decryption Keys) the primary tradeoff is mandatory registration of keys vs. no required registration of keys. Registration of keys would require the establishment of procedures and practices for the registration, storage, and retrieval of keys, as well as fines for improperly registered keys. This would require personnel, storage equipment/media, and maintenance of records. This cost would have to be weighed against the benefits. The primary benefit of mandating key registration would be to aid in law enforcement. A secondary benefit might be to deter criminals from committing crimes. In order to assign a value to this benefit one could consider the cost of crime and the possible reduction in that cost by using key registration instead of other surveillance techniques and the possible reduction in the cost of crime by deterrence. Risks of implementing mandatory key registration could include the misuse/unauthorized use of key and private communication information by law enforcement agencies, or possibly by telephone company employees.

The issues for Scenario Six (Export Controls on Cryptography) have been discussed several times by the Government (NSA, in particular) and by manufacturers of U.S. cryptographic equipment [59]. The primary tradeoffs are (1) export controls on all strong cryptographic technology, (2) no export controls on cryptographic technology, and (3) limited control on the export of cryptographic technology. The usefulness of the U.S. export restrictions on strong encryption technology has been debated several times [30,59] . The benefit of the U.S. policy on restricting technology that is already fairly readily available overseas has been questioned [26]. The potential economic benefit to U.S. manufacturers of lifting the export ban has been brought to the attention of law makers [13]. The cost of lifting the export restrictions has not been well defined. Factors would involve the cost incurred to national security agencies by the loss of surveillance. This could impact the U.S. in the form of terrorism, drug trafficking, organized crime, and the loss of military surveillance. The economic benefit of lifting the ban of export controls is also not well-defined, since the primary benefit, potential U.S. sales overseas, is not established. Some foreign manufacturers have begun selling encryption devices, and the potential for a large cryptographic market seems to exist. Since the impact of several factors is unknown, parametric analyses can be performed to assist in determining the costs,

risks, and benefits of lifting the ban on strong encryption technology exports. A parametric analysis was performed based on the percent of U.S. market share prevented based on a $100,000,000 market in encryption technology overseas.

5.0 Parameters Involved in Tradeoffs

General parameters important to several issues were identified in an effort to construct a generic, modular model applicable to most issues in digital telephony. Important aspects of issues in general were induced from the six issues analyzed here. Applicable parameters were determined with regard to cost elements involved in tradeoffs. Most of these cost elements could be used to model several communication issues. For example, cost elements used for the six scenarios analyzed include:

Cost Category:
- Equipment Installation Costs
- Equipment Maintenance Costs
- Equipment Operational Costs
- Value of Market Share

Risks Category:
- Cost of Misuse of Capability (Unauthorized Access/Use)
- Cost of Re-engineering
- Percent of Market Share Eroded
- Compromise of Sensitive Information
- Loss of Trade Secrets/Competitor Advantage
- Sabotage/Loss of Valuable Records
- Cost of Security Breakage

Benefit Category:
- Reduction in Amount of Crime
- Reduction in Police and Court Costs
- Reduction in Prison Costs
- Reduction in Specific Cost of Crimes
- Value of Crime Prevented
- Authentication of Information

Each of these cost elements could be applicable to a number of different issues. Specific parameters and values for each of these cost elements is implementation-dependent for each issue. For instance, in the 'Cost Category', equipment installation costs, maintenance costs, and

operational costs apply to Scenarios One, Two, Three, Four, and Five, and obviously could apply to several issues where the cost of communications equipment factors into a communications issue. Value of market share and percent of market share eroded are applicable to Scenario Six, dealing with export controls on cryptography, and would also be applicable to a technology tradeoff for a communications manufacturer involved in research, design, development, and manufacturing of new products. In the 'Risk Category', the cost of misuse of capability (unauthorized access/use) and cost of re-engineering apply to issues that involve implementing added features or capability to communication systems, as in Scenarios One, Two, Three, and Four. The additional cost elements in the 'Risk Category' above, compromise of sensitive information, loss of trade secrets/competitor advantage, sabotage/loss of valuable records, and the cost of security breakage pertain to issues analyzing the requirement for security (or the risks of inadequate security measures) such as Scenarios One, Two, and Four. The cost of security breakage might include as parameters the cost of repairing damage and the cost of adding additional security features. In the 'Benefit Category', the cost elements dealing with the cost of crime apply to Scenarios Three, Four, Five, and Six. Authentication of Information pertains to Scenarios One, Two, Four, and Five. Thus, several cost elements and parameters, and in some cases values, are generic to the analysis of several communication issues.

For each tradeoff certain primary considerations were investigated. Primary considerations included reliability, privacy, security and law enforcement considerations. Some general considerations for each of these aspects to the technical and policy issues are described below.

5.1 Reliability

Recently, Sandia National Laboratories and the Intel Corporation set a new record of 143.4 GFLOPS on the Massively Parallel LINPACK benchmark. [52] Sandia's Intel Paragon XP/S 140 supercomputer has 1840 computer nodes. Dr. Art Hale, Manager of Parallel Computing Science at Sandia, stated that with the given architecture, they had probably attained as many nodes as is possible "from a reliability point of view" [52]. As the telecommunications industry tries to push the state of the art, reliability is a key factor in determining associated costs and in determining the range of applications that can be supported. In the area of massively parallel supercomputing, reliability and accuracy is of utmost importance, as the merit of the entire system relies on sound, accurate computational results.

In the telecommunication area reliability often gives way to throughput (i.e. bandwidth or capacity). For example, ATM (asynchronous transfer mode) allows greater utilization of channel capacity by multiplexing several users onto one channel. The overall traffic rate at a particular point in time may be greater than the channel capacity [1]. Data could be lost as a result of this "data overflow". Techniques to deal with the problem of congestion in ATM networks are being sought [1], the most common of which is buffering. In order to be reliable, buffers must be able to store enough data to account for any overflow (on the order of megabits), and must employ logic fast enough to meet the timing requirements of ATM speeds (up to Gbps for some possible implementations) [1]. When designing for applications requiring low data rates and with well known statistics (such as voice), ATM could be used to multiplex several (approximately 20) calls on the same channel with relatively small impact on communicating parties [32] . On the other hand, latency (i.e., delay) has a significant impact on voice communication [32]. Voice communication must be transferred with fixed, minimal delay in order to be intelligible. Therefore, ATM networking must address the latency requirements for voice to provide reliable voice communication.

In order to provide reliable communication for multiple services using ATM, various design criteria must be met for individual applications. In addition to latency considerations for voice, bit error requirements for data and stringent timing and dynamic capacity requirements for video must be addressed. Providing reliable transfer for these varied applications could require several layers of re-engineering from the physical equipment and media to the applications level. In other words, the degree of reliability required for a telecommunication network directly affects the complexity of the design, and also therefore, the financial costs involved. This is the primary reason that military communication systems tend to cost an order of magnitude greater than commercial networks to implement. In addition to meeting the various timing, latency, and error correction criteria required for various types of communication traffic, Government applications often require greater accuracy of information and greater protection (or security) of that information. A non-reliable communication system in the sense of accuracy and security could have a severe impact on programs of national interest (and possibly even on the lives of U.S. citizens).

The costs for many complex, advanced, and highly reliable communication systems depend on basic research. It is difficult to predict the payoff of basic research. Obviously, some of the most important discoveries have been the result of basic research and have

impacted several areas in unexpected ways. For example, the work of Jerome Karle, Nobel laureate, in his research into DNA structures impacted the medical diagnoses of several diseases and also unexpectedly impacted several other research fields (i.e., synthetic fiber and other material developments) [35]. Even though financial tradeoffs in basic research are almost impossible to perform, the benefits of basic R&D (research and development) have more than paid for the costs for many projects in the Government and for many businesses. With the advancements in telecommunications technology, basic research must be performed in some areas before the engineering tradeoffs are known. Once those tradeoffs are known, a model, such as the 'Digital Telephony' model, can be used to compare the financial benefits of various implementations. Innumerous possible tradeoffs could be made for various issues and implementations of technology for the National Information Infrastructure. The entities examining telecommunication standards, policy, technology, developments and manufacturing include service providers, telecommunication hardware and software providers, and Government agencies. Reliability is a major concern as telecommunication capabilities advance. The reliability of the entire National Information Infrastructure depends on communication hardware/software performing as expected, interfacing reliably with other communication devices, and adhering to developed standards. As these various players in the implementation of the National Information Infrastructure devise new methods of implementing communications to meet the future telecommunication needs and manufacture various pieces of equipment, reliability should play a key role in deciding standards for devices, protocols, practices, and procedures.

The technical design and implementation of communications equipment to reliably and securely establish connections and transfer information is, therefore, a primary concern. Reliability includes having adequate resources such as bandwidth, error detection/correction, distributed networks, strong encryption and physical level security, and reliable equipment and media. This can have a significant impact on the cost consideration for a business or agency, and a value could be assigned to the importance of reliable communications in the operation of various communication services. This could also effect the required level of design of equipment. For instance, designing wiretaps into equipment (analyzed in Scenario Three) would require the re-engineering of communication equipment and development of advanced optical and switching techniques that would allow wiretaps to be efficient, effective, and non-intrusive (in other words, reliable). The 'Digital Telephony' model could be used to determine a reasonable amount of funds to be spent on

R&D research to examine possible means of implementing a tap capability. This could be based on the calculated benefit of wire taps and the calculated cost of using alternative surveillance methods.

In Scenario One (Security Implementation Tradeoffs), reliability is an important factor. Often, making a system more reliable requires adding redundancy and/or additional features, invariably enhancing the complexity of the system. Thus, the required degree of reliability could directly impact the overall cost. For example, in Scenario One a security tradeoff might be encryption/decryption techniques alone vs. encryption/decryption techniques with notification of physical interruptions in data flow. The first side to the tradeoff (encryption/decryption techniques alone) might provide security against the majority of attacks, while the second side to the tradeoff (encryption/decryption techniques with notification of physical interruptions in data flow) might provide added protection against attacks from insiders. For example, suppose someone with access to the encryption/decryption keys wanted to gain access to privileged information. A typical technique would be to tap into the communication channel. In a digital transmission system, if every instance of interruption in data flow must be accounted for, then this type of attack could be thwarted.

In Scenario Two (Initial Security Installation vs. Retrofit of Security Capability) reliability could be a cost factor indirectly. For instance, if one waited to implement security, an attacker could identify the protocols being used and later use the protocol information to aid in an attack against the encryption/decryption security. Any information regarding typical communications, especially protocol information, could greatly aid in deciphering cipher text. For example, an outsider observing the transfer of information on a network might easily identify the traffic as TCP/IP based on traffic patterns, even if the protocol was encrypted over a leased line. Knowing that information would convey a significant amount of plain text information that could be correlated with the encrypted information (allowing a "known-plain-text" attack). Therefore, reliability could be assigned a cost value in the benefit category for implementation of security during an initial communication system implementation.

In Scenario Four (Implementation of the 'Clipper Chip'), determining the degree of reliability of the system and the associated cost values could be quite complex since it would be a multifaceted variable. For instance, reliability could be considered with regard to systematically

attaining the proper keys for deciphering communications and also with regard to ensuring keys are only used for official purposes. These would in turn depend upon procedures being properly implemented at several stages of the key escrow system from device manufacturing to key storage to key retrieval. This type of analysis would also apply to the issues in Scenario Five (Registration of Keys) where not only do keys need to be reliably stored and retrieved, but so do the encryption/decryption algorithms for a set of keys.

5.2 Privacy

Privacy affects the ability of individuals/organizations to carry on communication and correspondence without disclosure of information to unauthorized or unwanted parties, and the degree to which personal and corporate information can be protected. It can be affected by the reliability and security of communication equipment, and the ability of telephone and government agencies to control and protect communications equipment. Of course, the ability of telephone and government agencies to control communication could adversely affect privacy. Privacy rights organizations, such as the ACLU (American Civil Liberties Union) promote the rights and interests of the individual (in contrast to national or societal rights). Individual rights groups believe that each person should be able to communicate privately with confidence that their private communication is not being listened to by outsiders. Given the forcefulness with which some news agencies pry into people's lives, it is understandable that some organizations distrust the use of a common single encryption/decryption system for everyone (such as the 'Clipper Chip', analyzed in Scenario Four). Even if the encryption/decryption algorithm is secure, the possibility of unauthorized eavesdropping or unauthorized disclosure of keys and/or communications could exist within an established system. The range of possibilities include unauthorized disclosure of keys by a manufacturer of a 'Clipper Chip' device to the unauthorized disclosure of communications during or after an authorized tapping of communications. The fact that this type of exploitation could be extremely difficult to detect is particularly disconcerting. Also, if a single encryption system was mandated, several parties might be interested in finding vulnerabilities in such a system (for instance, criminal defense lawyers, terrorists, drug traffickers, foreign governments, arms dealers (including nuclear), etc.).

The mandatory registration of keys, allowing individuals to use any cryptographic device but requiring the registration of all keys, is

considered in Scenario Five. This policy also brings skepticism concerning the proper use of key material by all persons who might come in contact with key material. Strict accounting procedures and fines would not alleviate the fear of misuse since insiders might circumvent accounting procedures and fines do not always provide a deterrent. (For example, minors can often find someone to buy them liquor despite fines imposed on those who sell liquor to a minor.) In order to pass legislation requiring key registration or mandating the use of the 'Clipper Chip', agencies must adequately address these privacy issues.

Scenario Three (Legislating Communication Equipment Wire-tap Capability) also affects the privacy of individuals, though the FBI has stated that they are trying to maintain present monitoring capabilities in the face of technological advances. Although this proposal was fervently attacked by privacy rights advocates, this proposal was defeated primarily because of the complex re-engineering involved and because of the detriment to the advancement of telecommunications capability it imposed.

5.3 Security

Security affects private records such as personal medical information, tax records, assets, as well as corporate records such as banking transactions, trade secrets, and proprietary information, and sensitive Government information. These records, if not secured, could be obtained and used in crimes ranging from robbery and blackmail to abduction, murder, plagiarism, terrorism and espionage. Security must be implemented at various levels, from the applications layer to the network management layer to the physical layer. (The Open System Interconnection (OSI) standard defines seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Applications Layers [7].) From a network management point of view, protocols must be constructed to be unambiguous and to place the network in clearly defined states. The network management procedures, protocols, and signaling information must be safeguarded and access to the control of network services must be protected. Also, any added features, physical characteristics, and logical and physical connections must be implemented so that security is not compromised. For instance, call forward must be designed so that communication between two parties cannot be forwarded without their knowledge and consent. New features, such as call forwarding, caller I.D., teleconferencing, central message recording, are continuously being added to telephone services. As new features are designed, they must be

scrutinized to ensure that communication security is not diminished, particularly by making call set-up and control too generic or too accessible.

Besides network management issues, security must also be addressed at the user level, including encryption of sensitive communications. The level of security required directly affects the costs, risks, and benefits of the resulting telecommunication security system. Security can be implemented at the physical layer by providing 'impenetrable' equipment (or tamper resistant/evident devices with built-in alarms), by the network layer by switching and routing principles, by the applications layer by cryptographic techniques, or by other layers. (Data Link, Transport, Session, or Presentation Layers [7].) The level of security in a network might require redundancy, and so security at several layers might be implemented. The ease of detection of security violations, and the risks of security breakage can be assessed and assigned cost values in relative terms by comparing various systems.

Often, military and civilian Government communication systems require greater security than that offered by the telecommunications providers. The issues dealt with in Scenarios One and Two, security implementation tradeoffs, and initial installation vs. retrofit of security capabilities could apply to tradeoffs involving various media, communication platforms, communication frequencies, and other communication equipment. The cost considerations between alternate approaches could be considerable. With Vice President Al Gore's initiative for 'right-sizing' (down-sizing) Government [55], many possible tradeoffs should be analyzed. Additional scenarios address and supply parameters for evaluating issues affecting national security interests such as surveillance capabilities. Often, national security interests directly contrast with individual and corporate security interests. Especially for those who question the integrity of the law enforcement process, access to individual and corporate communications by law enforcement agencies and national security agencies poses a threat to individual privacy. Scenario Three (Legislating Communication Equipment Wire-tap Capability), Scenario Four ('Clipper Chip' Implementation), Scenario Five (Registration of Keys), and Scenario Six (Export Controls on Cryptographic Technology) all address issues affecting the surveillance capability of national security agencies and law enforcement agencies. Possible subjective parameters are included in the 'Digital Telephony' database (e.g., compromise of right to privacy). These subjective parameters were not assigned values in the examples shown herein, but in exercising the model, one could assign comparative values to subjective parameters on

various sides of an issue. Additional considerations for Scenarios Four - Six are the ability of national security agencies and law enforcement agencies to bring criminals to justice, to interdict drug traffickers, to prevent terrorism, and to control the spread of nuclear technology.

5.4 Law Enforcement

Law enforcement concerns effect the ability of the Government to preserve law and order and to protect the interests of the United States of America. The efficiency of tools available to law enforcement agencies also effects the price paid by American taxpayers both for law enforcement costs and, in the case of inefficient tools, for crime costs. Often, the methods used by law enforcement agencies are necessarily very costly. Therefore, the cost of preventing crime, enforcing justice, and convicting criminals can have a tremendous impact in issues concerned with the ability of law enforcement agencies to effectively enforce the law. For instance, in Scenarios Four - Six, which all deal with initiatives to aid law enforcement, the benefits of implementation based on cost of crime figures is significant. Although the cost of implementation of several initiatives is considered significant, as in implementation of the 'Clipper Chip' and in implementation of B-ISDN wire-taps, the benefit derived from the prevention of crime typically outweighs the cost.

6.0 Database Construction

A generic database was constructed incorporating many known parameters. Related parameters were grouped into 'Cost Elements'. Cost Elements are grouped and identified for scenarios following each issue heading. The rows of the database are comprised of the individual parameters. Columns were constructed for (1) Cost Elements, (2) Parameters, (3) Metrics, (4) Requirements, (5) Parametric Parameters (parameters used in parametric-dependant analyses), (6) Starting Metric Values, (7) Ending Metric Values, (8) Step Values, and (9) Nominal Metric Values. Since not all parameters would apply for a particular issue, the 'Requirements' column is used to mark all parameters pertaining to a particular issue. All parameters exercised for a particular issue were noted by entering a '1' in the 'Requirements' column of the Digital Telephony Database. The model is designed to use the nominal value for computing the total cost for each side of an issue. When computing parametric costs, the 'Parametric Parameter' column is used to identify the parameter to be varied, and the parameter's values are varied

according to the 'Step Value' from the 'Starting Metric Value' to the 'Ending Metric Value'. Parameters used for parametric analyses were noted by entering a '1' in the 'Parameter Column'. The starting, step, and stopping values were entered for each of these parameters. 'Run-time buttons' were developed to exercise the command macros developed using Microsoft Excel to run the cost model and to construct parametric tables. A 'Run Model' button was implemented to select for running the model. A 'Run Parametric Table' button was implemented to select for constructing a parametric table and corresponding plot.

7.0 Equations, Parameters, and Dependencies

Cost equations were determined for each cost, risk, and benefit element and formulas were inserted in the appropriate cells to determine the total cost for each cost, risk, and benefit element. These formulas are specified in the tables for each issue. Note that current and accurate values for data and statistics must be obtained to evaluate any communication tradeoff, whether the tradeoff involves technical or political issues. For the examples given, research on parameters and values was limited to figures generally available [4,5,8,23,24,31,33,38,45,49,51,54,56], requiring an estimation for some parameter values. The analysis of certain industry experts was used as a basis for certain calculations (i.e., Robin Hanson's "Would Wiretap Chip Be Cost Effective?" in the case of proposed wiretapping implementation [31]). Several parameters and values have been incorporated into the Digital Telephony database constructed for use with the developed model.

The impact of most issues discussed herein is wide-ranging and, therefore, the total impact on related industries, policies, and procedures is difficult to assess. As a consequence the model is constructed so that additional parameters can easily be incorporated. Since the effect (or degree of effect) of certain parameters may be unknown, parametric analyses can be valuable by providing a means to test for the effect of varying the assigned values or varying the effect of the assigned value in the overall cost calculations.

In some cases a parameter used to produce cost estimates is highly variable. This may be because of changing markets, unknown effects of implementation, or other uncertainties. Estimates for the cases presented herein were obtained through reports on residential and commercial telephone line usage, and reports on crime statistics, including the estimated number of wire taps, prosecutions, convictions,

incarcerations, etc. for various classes of crime. Appropriate ranges of variance for key parameters were determined from general research (based on sources listed in Paragraph 3.0 above) and added to the Digital Telephony database. Highly variable or key parameters can be varied over ranges of possible values to provide parameter-dependent tables and plots, displaying the effect of changes and/or errors in the estimates.

8.0 Examples of Several Telephony Cases

The Scenarios outlined below include: (1) security implementation tradeoffs, (2) initial installation vs. retrofit of security capabilities, (3) legislating communication equipment wire-tap capability, (4) 'Clipper Chip' implementation, (5) registration of keys, and (6) export controls on cryptographic technology. Parameters were developed for each side of the issues and values were attached to each parameter. The model was exercised for each of these scenarios to provide example numerical and graphical results for the values used.

Scenarios Two, Three, Four, Five and Six each contain highly variable critical parameters. Therefore, parametric analyses were performed for each of these. For Scenario Two the percent of transmitter/receiver pairs modified to add security to communications was varied to show the point at which designing security into the system at the outset would be more cost effective. For Scenario Three parametric tables were computed for ranges of the cost of crime, as these values could vary and/or increase greatly due to increasingly more sophisticated criminal activities and involvement of organizations, companies, and even local government. For Scenario Four the probability that only the 'Clipper Chip' encryption was being used in cases a search warrant was obtained was varied from 0% to 100% in steps of 10%. For Scenario Five a parametric table was computed over the range of probability that keys were properly reported for cases in which legal intercept warrants were obtained. For Scenario Six the projected U.S. market share of the projected European cryptographic market was used to construct a parametric table of projected lost U.S. sales. The results for each tradeoff scenario follow.

8.1 Security Implementation Tradeoff

As stated above, common communications security equipment tradeoffs involve software vs. hardware solutions, physical level security vs. applications level security (as described in Paragraph 5.3 above), and

tradeoffs in encryption devices and algorithms. For instance, to use encryption/decryption for securing communications, a company might implement encryption/decryption algorithms using hardware devices or software. In a non-technical environment hardware devices might be preferred because of simplicity, although software encryption is usually less expensive. Running the digital telephony model with specific values for a particular instance would display the additional overall cost of using hardware encryption instead of software encryption.

Several aspects of possible tradeoffs between security systems are included in the digital telephony database, including initial system costs, maintenance costs, key storage and distribution costs. Different security systems might also have different risks associated with them. For instance, a security breach might require the replacement of a substantial amount of equipment. This type of cost would vary with each system. Also, some security systems might be more easily compromised than others, and this may depend greatly on the operation of the communication system and specific procedures in an organization. Parameters were developed to be generic with regard to the type of communication devices/systems under consideration, including benefits regarding the ease of detection of security violations and including risks of security breakage. A sample case was modeled using the digital telephony model and the results are given.

In this scenario the communications security for a bank with several branches is considered. The primary type of information to be protected is data in the form of personnel and corporate banking transactions. Authentication, integrity, and confidentiality of these data transactions must be maintained. Since important transactions are handled by computers, security of the computer communications across a wide area network (WAN) is one of the primary concerns. The need for secure FAX communications also exists. One secure voice line is required for banking customers to dial into to obtain account information. Additional secure voice lines may be required in the future to allow banking customers to make transactions by phone, including purchases made from home over the telephone or cable network.

Security must be implemented at various levels, from the applications layer to the network management layer to the physical layer. The network management procedures, protocols, and signaling information must be safeguarded and access to the control of network services must be protected. Encryption of information is becoming a common means of securing communications. However, encryption alone does not necessarily

provide secure communications. For example, if standard protocols are used, encryption of the protocol could provide valuable information to a hacker attempting to decipher text, increasing the amount of plain text that is known. (Someone familiar with standard protocols could determine the plain text for given cipher text and possibly use that information to determine the key.) In addition, the physical security of communication equipment and media must be considered. Access to the communication equipment must be controlled and notification of any disruption of data traffic must be provided (as this might be evidence of an attack on the data in route from source to destination).

The primary tradeoff analyzed in the following text is hardware vs. software encryption of voice, data, and fax communications. Implementation of encryption algorithms in hardware tends to drive up the cost of implementing encryption/decryption procedures (as can be seen by comparing the cost of 'Clipper Chip', estimated at $30 [42], with the cost of the RSA algorithm, $0 [46,47]; the 'Clipper Chip' cost estimation was provided before a flaw was discovered, requiring the re-manufacturing of all chips). Software encryption/ decryption devices tend to cost less but require greater maintenance costs. Maintenance costs might include installing and reinstalling software on new platforms, maintaining the software, ensuring operability under new operating system releases, and maintenance of the associated computer equipment. Other indirect cost figures are associated with different forms of implementation. For example, benefits of hardware encryption include portability. This might reduce the number of cryptographic devices needed. Another benefit of hardware encryption might be greater accountability for keys, as some type of "physical" key is typically used for hardware encryption (linking an individual to a compromised key), as opposed to a software key entered in the code or at the keyboard (possibly involving many individuals). In the case of a security breakage and sabotage, the additional risk costs when using hardware encryption/decryption outweighs the additional risk costs when using software encryption/decryption. For instance, compromise/sabotage of hardware encryption devices could entail the replacement of hardware (possibly all hardware), because of tampering. In the case of software encryption, the original software can be re-installed. (Even in the case of viruses, a previous system back-up could be downloaded.) The most common risk is unauthorized disclosure of keys (in which case new keys could be obtained and/or downloaded). If encryption/decryption keys are compromised, the risk factors for both hardware and software encryption would include loss of proprietary information and loss of data integrity.

The values used for the various costs are shown in Table 1. These values are used for illustrative purposes in order to exercise the model, as actual cost values for software and hardware can fluctuate. It is assumed that software encryption products will be loaded on existing platforms (probably computationally intensive workstations), and will not be portable, whereas hardware encryption products will be self-contained and portable, requiring less units to be purchased. As can be seen, the initial implementation cost for the first set of equipment, hardware cryptographic equipment, ($6,500) is greater than the initial implementation cost for the second set of equipment, software cryptographic equipment, ($2,500). However, the maintenance costs of the first set of equipment ($150/year) is less than the maintenance costs of the second set of equipment ($10,000/year). The risks associated with the first set of equipment ($3,000) is greater than the risks associated with the second set of equipment ($500) because of the greater cost of replacing sabotaged equipment for hardware-based cryptographic equipment. The benefits of the hardware-based cryptographic equipment ($3,040) are greater than those of the software-based cryptographic equipment ($1,500) because of the transportability of the hardware devices and greater accountability of hardware equipment and encryption/decryption keys. The benefit of hardware device portability is given a relative value based on additional portability over software and an associated computer system. The total cost of using the hardware cryptographic system in this example scenario is $6,650 compared to the total cost of $12,500 for the software cryptographic system. Factoring in the risks and benefits of each approach, the cost of hardware encryption/decryption is $5,610 and that of software encryption/ decryption is $11,500, as shown in Table 1 and Table 2 (generated by the model). The risks and benefits associated with hardware cryptographic equipment have greater dollar values than that of software cryptographic equipment. Since the value of the benefits are subtracted from the costs and the value of the risks are added to the costs when both are considered, the overall impact of including the indirect costs associated with the risks and benefits is small. In this scenario the overall cost of using hardware is less than the overall cost of using software, primarily due to the increased costs of maintaining software (though many other factors have some impact).

The costs included in this example scenario are linearly dependent. Sometimes the cost of the number of hardware devices or the number of software licenses is non-linear with respect to the number of units. This would have minimal impact on the overall costs since this is typically a very slowly decaying exponential, but this non-linearity could easily be

modeled by subtracting a value based on the number of units, or including look-up tables or other non-linear models when they are known.

TABLE 1: SECURITY IMPLEMENTATION TRADEOFF MODEL

Side One - Hardware Implementation					
Side One Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Cost of First Set of Equipment	Cost of Each Complete Unit	dollars/unit		200	
	Number of Units	integer		20	
	Total Cost of Units	dollars	Cost of Each Complete Unit* No. of Units	4,000	4,000
	Total Cost of Installation	dollars		2,500	6,500
	Total Cost of Maintenance/ Year	dollars		150	6,650
Side One Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Cost of Security Breakage With Equipment Set No. 1	Cost of Repair-ing Damage	dollars		3,000	9,650
	Cost of Adding Additional Security	dollars		0	9,650
Side One Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Benefits of Using Equipment Set No. 1	Prevented Value of Lost Information	dollars		0	9,650
	Saved Labor Hours	hours/year		52	
	Average Cost per Labor Hour	dollars/hour		20	
	Total Labor Cost Saved	dollars	Saved Labor Hours*Average Cost per Labor Hour	1,040	8,610

	Prevented Personal Information Leakage Costs	dollars/year		2,000	6,610
	Saved Legal Fees	dollars/year		1,000	5,610
Side Two: Software Implementation					
Side Two Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Cost of Second Set of Equipment	Cost of Each Complete Unit	dollars/unit		50	
	Number of Units	integer		40	
	Total Cost of Units	dollars	Cost of Each Complete Unit* No. of Units	2,000	2,000
	Total Cost of Installation	dollars		500	2,500
	Total Cost of Maintenance/ Year	dollars		10,000	12,500
Side Two Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Cost of Security Breakage With Equipment Set No. 2	Cost of Repair-ing Damage	dollars		500	13,000
	Cost of Adding Additional Security	dollars		0	13,000
Side Two Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Benefits of Using Equipment Set No. 2	Prevented Value of Lost Information	dollars		0	13,000
	Saved Labor Hours	hours		0	
	Average Cost per Labor Hour	dollars/hour		0	
	Total Labor Cost Saved	dollars	Saved Labor Hours*Average Cost per Labor Hour	0	13,000
	Prevented Personal Information Leakage Costs	dollars		1,000	12,000
	Saved Legal Fees	dollars		500	11,500

SECURITY IMPLEMENTATION TRADEOFF
TABULAR RESULTS

ISSUE 1: SECURITY EQUIPMENT TRADEOFF
SIDE 1: Security System Number 1 (Hardware Implementation)
SIDE 2: Security System Number 2 (Software Implementation)

SIDE_NUMBER	TOTAL_COST
1	5,610
2	11,500

Model Result: Security System Number 1 is More Cost Effective
In this analysis the initial high cost of system number 1 is offset by the higher cost of maintaining system number 2.

Table 2

Innumerous variations of this scenario can be analyzed. For instance, suppose the cost of adding stronger encryption was analyzed. Advancements in ASIC (Application-Specific Integrated Circuit) technology and supercomputing limit the life of any encryption scheme. Estimates can be determined for the amount of computational power and time required to break the encryption/decryption key. Often, stronger encryption can be provided by adding feedback loops to take the ciphered (encrypted) text and run it through the encryption algorithm a second time (or even a third time). (Although this is true for several popular encryption devices, such as Triple DES (Data Encryption Standard), this might add no more strength than the original encryption and has also been known to weaken algorithms, depending on the encryption technique.) This can have a significant impact on the amount of computational power required to break the encryption/decryption key. (If one uses an exponential algorithm, the computational power required can increase by orders of magnitude.) So, for instance, a variation to this scenario might analyze the additional amount of computer and personnel resources required to analyze and add feedback loops to the encryption process vs. the resources (hardware/software/key generation and storage, etc.) required to upgrade to a new (stronger) encryption device. Additional tradeoffs could compare various media, communication platforms, communication frequencies, and other communication equipment.

8.2 Initial Design With Security vs. Retrofit

The high cost of implementing security into communication systems leads many businesses to delay adding security until a need arises and then to secure only certain systems/equipment. Often the cost of adding security later is greater due to some redesign and/or replacement of existing equipment. Also, adding security incrementally can be much more costly overall. If security requirements can be sufficiently anticipated, a financial tradeoff can be easily developed. The digital telephony database incorporates many of the parameters needed for such a tradeoff, and a sample scenario was modeled and executed.

This scenario considers a medium-sized business with international offices. The company has an R&D facility and develops new manufacturing designs and processes. (This could apply, for instance, to an automobile manufacturer or VLSI chip manufacturer.) The value of the company's proprietary information, which at times is communicated over the public network, is significant, and unauthorized disclosure of this information

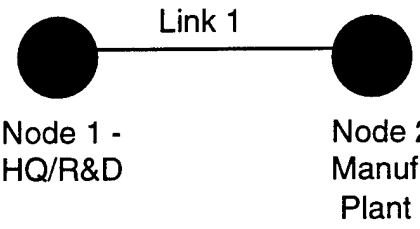
could cause the company to lose its competitive edge and potentially cause serious financial trouble. The company is not aware of any instance that proprietary information has been compromised during communication over the public network. The company is in the process of adding two new manufacturing facilities. The question of adding communication security equipment has been raised, but thus far, the need has not "been established", and adding communication security equipment has not been pursued.

Since the company is interested in the financial "bottom-line" and the need for installation of some type of communication security system at some point is highly probable, a financial trade-off of the costs associated with an initial installation vs. a retrofit of security capabilities is desirable. This tradeoff is complicated in this scenario by the need to retrofit existing offices with communication security capabilities if the new manufacturing facilities are equipped with communication security capability. Network connections for the new and existing facilitites are displayed in Figure 1aa. Secure communication will be required between the R&D facility (located at the business' headquarters) and the existing and new manufacturing facilities. Although the existing communication 'centers' (which would require retrofitting if security is added to the new facilities) constitute 50% of the total communication facilities, the communication equipment requiring retrofitting constitutes less than 50% of the communication equipment (assuming transmitting and receiving pairs required between each pair if nodes). Since secure leased lines would be desirable between each of these four locations, 16.7% of the communications between facilities would require retrofitting even if security is installed at the new facilities at the outset. This is calculated using the following formula:

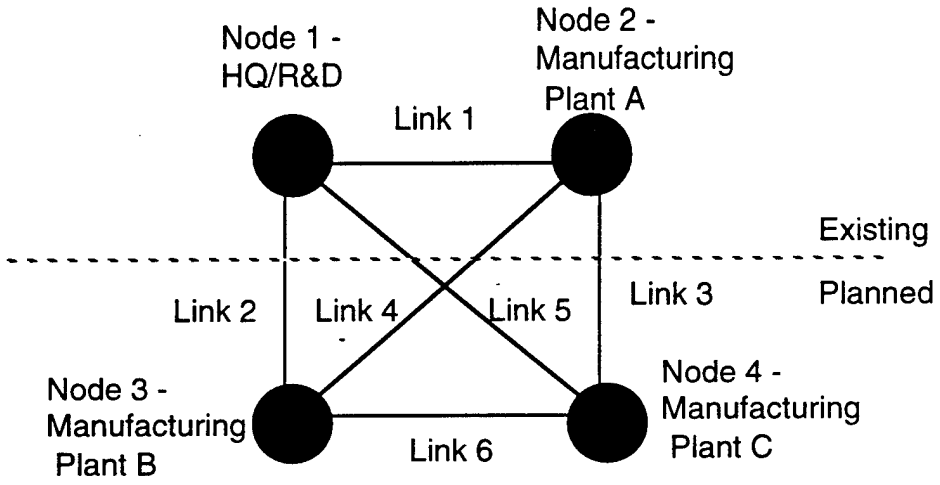
Number of Links = SUM (i=1 to n) of (i-1) where n=Number of Nodes

For example, 1 link exists between two nodes and six links exist between four nodes as shown in Figure 1aa. One divided by six equals 16.7%. Therefore, for this scenario the cost of retrofitting 16.7% of the total communication system with security capabilities must be added to the cost of an initial security installation of 50% of the communication system. This is compared to the cost of retrofitting 100% of the communication system with security capability at some point in the future. Initial security installation is considered as Side One and retrofit of security capability is considered Side Two.

FULLY CONNECTED NODES



a. Two Nodes Fully Connected -
Existing Nodes and Links



b. Four Nodes Fully Connected -
Existing and Planned Nodes and Links

Figure 1aa

Due to the nature of business operations it is decided that three secure voice lines between each facility and four secure modem lines (three for computers and one for faxes) will be required/multiplexed on each link. Security measures will include leased lines, error detection/notification, and encryption of all traffic. It is assumed that leased lines are available in other countries where factories are located. Leased lines also guarantee a certain amount of bandwidth, so that when design files are transferred, information will not be lost because of congestion. Since leased lines are to be used, a unique protocol could be developed to minimize information revealed about the plain text, along with a protocol translation device to interface between the transmission

media and standard communication devices. A 'black box' could be used on each end of the transmission (i.e., at each facility) to handle protocol translation and communication. After adding a CRC (cyclic-redundancy-check), the communication traffic will pass through the 'black box' for protocol encapsulation, and then the encryption device. On the receiving end the communication traffic will be decrypted, the protocol header information stripped off, and the CRC performed to detect errors. If errors are detected, notification will be sent, along with the number of bits affected. This provides a 'data-integrity' check to determine if data has been modified.

The primary cost factors and values: cost of initial installation, retrofit of existing equipment, and cost of maintenance are shown in Table 3, along with other cost factors. Engineering labor is required to design a proprietary protocol for company use. Encryption and information coding and decoding (CRC implementation) are available as commercial off-the-shelf hardware. Maintenance costs include labor hours for maintaining communication equipment and ensuring proper operation of the information coding, protocol operation, and encryption/decryption of communication traffic. Representative values were assigned to the various cost parameters to execute the model for illustrative purposes. As can be seen in Table 3, the direct costs associated with an initial installation are $398,700, while those associated with a retrofit of equipment are $368,100. The indirect cost associated with the risks of an initial installation are zero dollars, while those associated with a delayed installation are $210,000. Of course, the indirect costs associated with potential risks can be significant and are highly dependent. The risks in this scenario are considered greater than the risks for communication strictly in the continental United States. The indirect cost as associated with the benefits of an initial installation are $20,000, while those associated with a delayed installation are zero dollars. An indirect benefit derived from the installation of secure communications considered in this scenario is the reliable transfer of design files used in the manufacturing process. The sum of direct costs and risks minus benefits for an initial installation are $378,700, while those for a delayed installation are $578,100, as shown in Table 3 and Table 4 (generated by the model). The cost of a delayed installation and resulting retrofit of communication equipment is 50% greater (or 1.5 times greater) than an initial installation.

The associated risks and benefits are somewhat complimentary. For instance, the risks of delayed installation of security could be considered instead as the benefits of initial installation of security. If reduction in

TABLE 3: INITIAL DESIGN WITH SECURITY VS. RETROFIT MODEL

Side One: Initial Security Implementation					
Side One Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation of Security Capability (Initial)	No. of Receivers/ Transmitters	integer		42	
	Added Cost per Receiver/ Transmitter	dollars/ receiver & transmitter		5,000	
	Total Receiver/ Transmitter Cost	dollars	No. of Receivers/Transmitters*Added Annual Cost per Receiver/ Transmitter	210,000	210,000
	Annual Added Operations Cost	dollars/year		20,000	230,000
	One-Time Design/Development Cost	dollars		10,000	240,000
Utilization of Security Capability (Initial)	Key Generation/ Distribution (Initial)	dollars		8,400	248,400
	Key Generation/ Distribution (On-going)	dollars/year		4,200	252,600
	Key Management	dollars/year		8,400	261,000
	Key Storage	dollars/year		2,100	263,100
Additional Maintenance	Additional Years Maintained	years		3	
	Additional Cost	dollars	Additional Yrs. Maintained* (Added Annual Operations Cost +KeyGen/Distr. Ongoing + Key Management + Key Storage)	104,100	367,200
Depreciation For Initial Installation	Depreciation	dollars/year	Total Receiver/ Transmitter Cost*0.05	10,500	

	Total Depreciation	dollars	Depreciation * Additional Yrs. Maintained	31,500	398,700
Side One Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Compromise of Sensitive Employee Information	Cost of Legal Services	dollars/year		0	398,700
	Cost of Lost Suits	dollars/year		0	398,700
Loss of Trade Secrets/Competitor Advantage	Lost Profits	dollars/year		0	398,700
	Cost of Legal Services	dollars/year		0	398,700
Sabotage/Loss of Valuable Records	Cost of Losses	dollars/year		0	398,700
Side One Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Authentication of Information (Apriori)	Value of Correct Information (Reliability)	dollars/year		20,000	378,700
Side Two: Retrofit of Security Capability					
Side Two Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation of Security Capability (Retrofit)	Number of Receivers/ Transmitters	integer		42	
	Percent of Receivers/ Transmitters	percent		1.0	
	Cost to Modify Each Receiver/ Transmitter Pair	dollars/ receiver & transmitter		7,500	
	Total Modification Cost for Receivers/ Transmitters	dollars	No. of Receivers/Transmitters*% of Receivers/ Transmitters* Cost to Modify Each Receiver/ Transmitter	315,000	315,000

	Added Annual Operations Cost	dollars/year	IF(No. of Receivers/Transmitters *% ofReceivers/ Transmitters>0, 20000,0)	20,000	335,000
	One-Time Design/Development Cost	dollars	IF(No. of Receivers/Transmitters *% ofReceivers/ Transmitters>0, 10000,0)	10,000	345,000
Utilization of Security Capability (Retrofit)	Key Generation/ Distribution (Initial)	dollars/ receiver & transmitter		200	345,000
	Total Key Generation/ Distribution (Initial)	dollars/year	Key Generation/ Distribution (Initial)*No. of Receivers/ Transmitters* % of Receivers/ Transmitters	8,400	353,400
	Key Generation/ Distribution (On-going)	dollars/year/ receiver & transmitter		100	
	Total Key Generation/ Distribution (On-going)	dollars/year	Key Generation/ Distribution (On-going)*No. of Receivers/ Transmitters* % of Receivers/ Transmitters	4,200	357,600
	Key Management/ Receiver/ Transmitter	dollars/ receiver & transmitter		200	
	Total Key Management	dollars/year	Key Management/Receiver/ Transmitter* No. of Receiver/ Transmitters* % of Receivers/ Transmitters	8,400	366,000
	Key Storage/ Receiver/ Transmitter	dollars/ receiver & transmitter		50	

	Total Key Storage	dollars/year	Key Storage/ Receiver/ Transmitter* No. of Receiver/ Transmitters* % of Receivers/ Transmitters	2,100	368,100
Side Two Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Compromise of Sensitive Employee Information	Cost of Legal Services	dollars/year		0	368,100
	Cost of Lost Suits	dollars/year		0	368,100
Loss of Trade Secrets/Competitor Advantage	Lost Profits	dollars/year		200,000	568,100
	Cost of Legal Services	dollars/year		10,000	578,100
Sabotage/Loss of Valuable Records	Cost of Losses	dollars/year		0	578,100
Side Two Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Authentication of Information (Aposteriori)	Value of Correct Information (Reliability)	dollars/year		0	578,100

INITIAL DESIGN WITH SECURITY VS. RETROFIT
TABULAR RESULTS

ISSUE 2: SECURITY DESIGNED INTO SYSTEM VS. ADDED LATER (COMMERCIAL)

SIDE 1: Security Designed Into System
SIDE 2: Security Added Later (25%)

SIDE_NUMBER	TOTAL_COST
1	378,700
2	324,525

SIDE 2: Security Added Later
PARAMETER: Percent of Receiver/ Transmitter Pairs Modified

SIDE_NUMBER	PARAM_VALUE	TOTAL_COST
2	0.00	210,000
	0.10	273,810
	0.20	307,620
	0.30	341,430
	0.40	375,240
	0.50	409,050
	0.60	442,860
	0.70	476,670
	0.80	510,480
	0.90	544,290
	1.00	578,100

Model Results: If 42% of Transmitter/Receiver Pairs Will Eventually be Required to Have Security Built-in, it is More Cost Effective to Design Security into the System at the Start.

ISSUE 2: SECURITY DESIGNED INTO SYSTEM VS. ADDED LATER (MILITARY)

SIDE 1: Security Designed Into System
SIDE 2: Security Added Later (25%)

SIDE_NUMBER	TOTAL_COST
1	1,827,700
2	797,025

SIDE 2: Security Added Later
PARAMETER: Percent of Receiver/ Transmitter Pairs Modified

SIDE_NUMBER	PARAM_VALUE	TOTAL_COST
2	0.00	210,000
	0.10	462,810
	0.20	685,620
	0.30	908,430
	0.40	1,131,240
	0.50	1,354,050
	0.60	1,576,860
	0.70	1,799,670
	0.80	2,022,480
	0.90	2,245,290
	1.00	2,468,100

Model Results: If 72% of Transmitter/Receiver Pairs Will Eventually be Required to Have Security Built-in, it is More Cost Effective to Design Security into the System at the Start.

Table 4

the loss of proprietary information/trade secrets and the associated legal costs is considered as a benefit, the cost plus risks minus benefits for initial installation is $378,700 - $210,100 (or $168,600).

As shown in this example scenario, some parameters have a fixed cost regardless of the number of units of equipment (eg., Added Annual Operations Cost and One-Time Design/ Development Cost in Table 3). When no units are purchased, however, these costs are zero. In order to 'zero out' these costs for zero units and maintain a fixed value for 1 or more units, an Excel Worksheet function is used as shown in Table 3. Most types of typical program statements are available as Excel functions. These functions can be used to provide logic operations within the worksheet/database as well as within the macros, creating additional extensibility.

A parametric analysis was performed to determine the percentage of transmitter/receiver pairs that could be retrofitted for secure communications for the same cost as initially installing secure communication for all transmitter/receiver pairs. A transmitter/receiver pair is considered to include the information coding/decoding, the protocol encapsulation, the encryption/decryption, and the cost of the leased line. The percentage of transmitter/receiver pairs was varied from 0% to 100% with Table 4 showing the cost increase as a function of the increase in percentage. As shown in Table 4 and Figure 1a, the transmitter/receiver pairs that can be modified at the later date for the same cost as initially installing secure communications for all transmitter/receiver pairs ($378,700) was calculated to be 42%. If all transmitter/receiver pairs will eventually be secured, the additional cost for adding security later could also be factored against the cost of financing the initial installation.

The cost associated with a military system might be an order of magnitude greater because of unique requirements and limited installations. This additional cost would be seen primarily in the implementation cost of the transmitter/receiver pairs. In this scenario, if this cost was just seven times greater per transmitter/receiver, the overall cost would be $1,827,700 for an initial installation and $2,468,100 for a 100% retrofit, as can be seen in Table 4 and Figure 1b. As shown in Table 4, for a military system the cost of retrofitting more than 72% of switches is greater than the cost of designing security into the system at the start ($1,827,700).

INITIAL DESIGN WITH SECURITY VS. RETROFIT (COMMERCIAL)
PARAMETRIC ANALYSIS

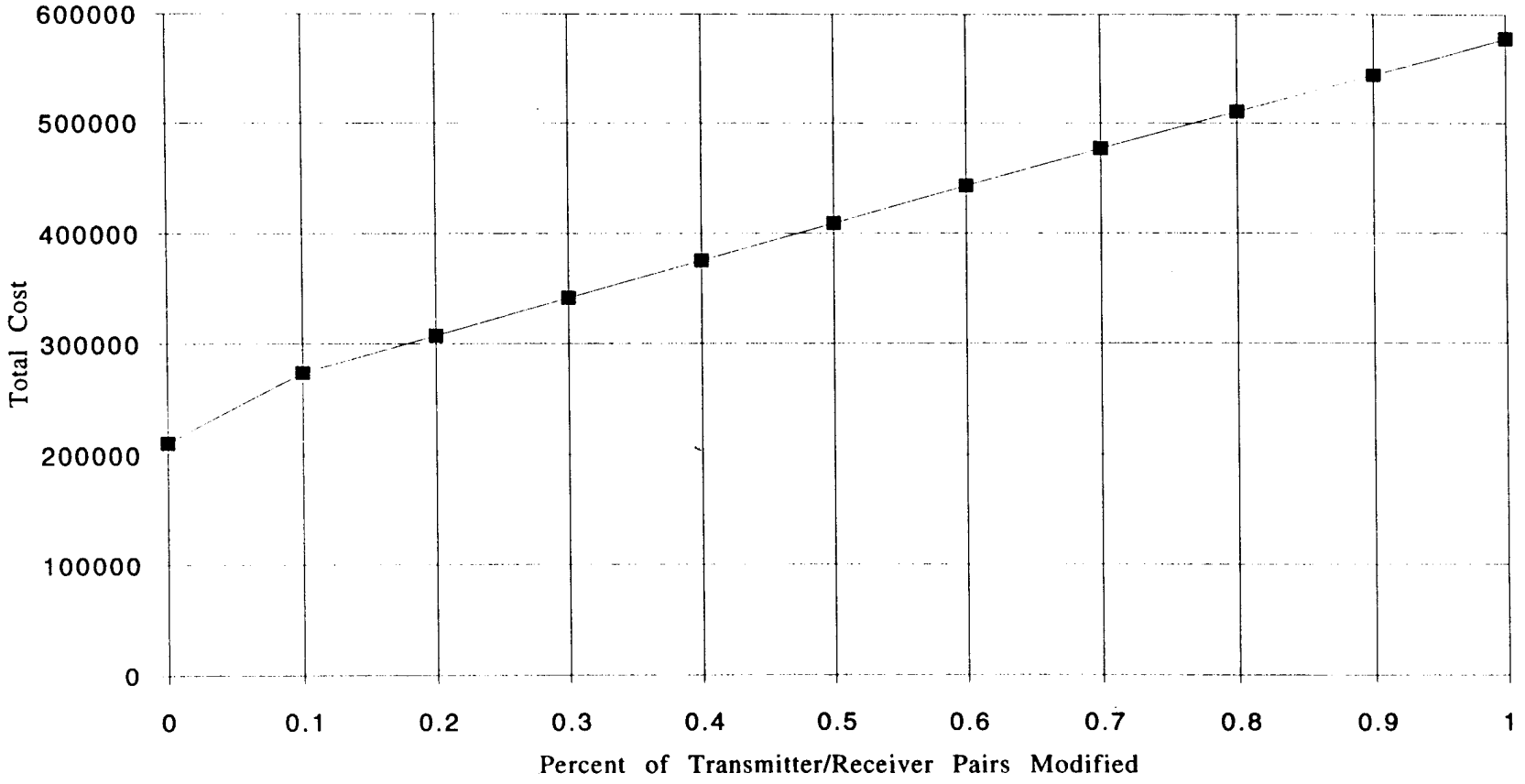


Figure 1a

INITIAL DESIGN WITH SECURITY VS. RETROFIT (MILITARY) - PARAMETRIC ANALYSIS

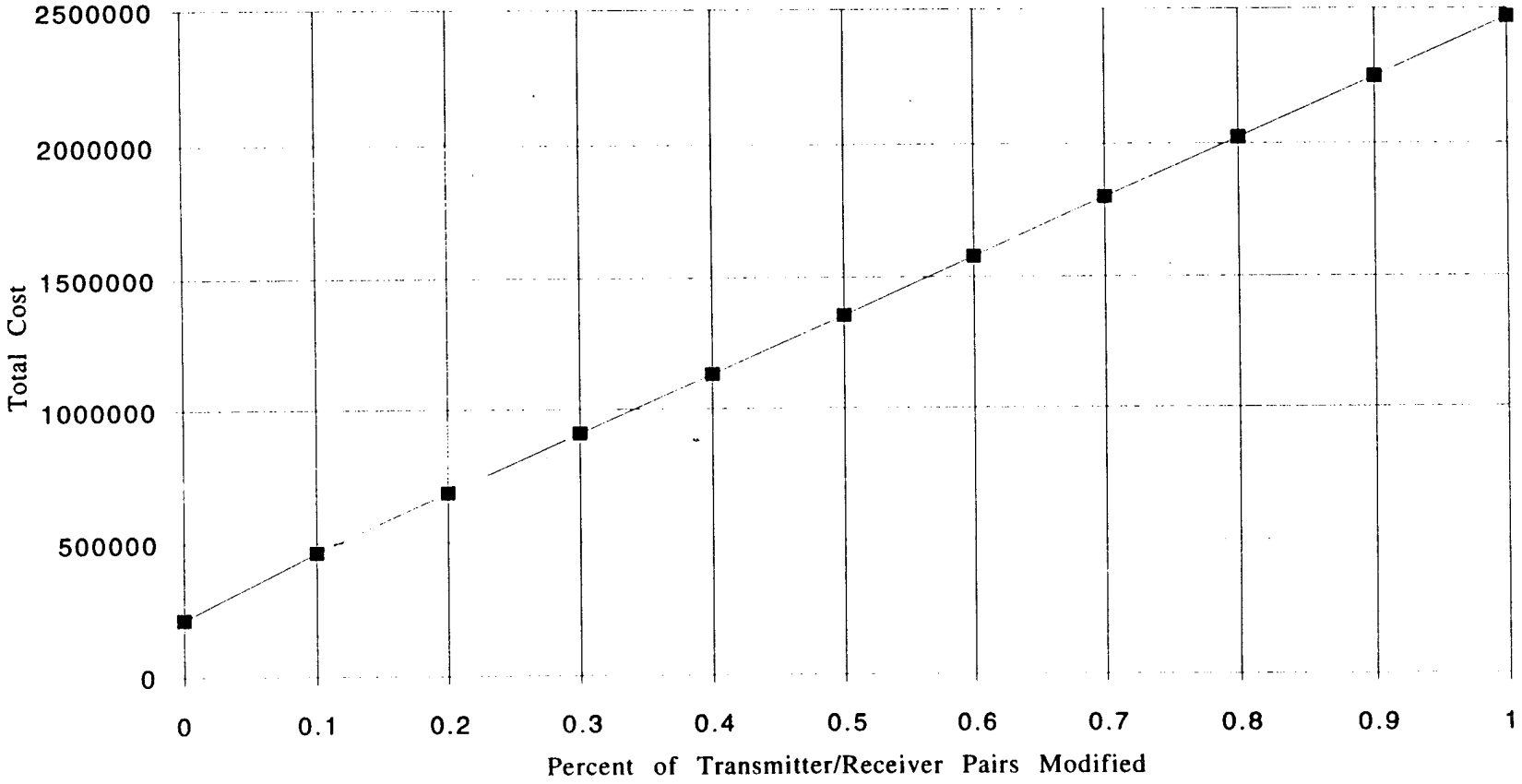


Figure 1b

Reliability is a major factor in determining the level of technical design and implementation of communications equipment. In this scenario many levels of safeguarding were used to establish highly secure and reliable communications. Several tradeoffs could be implemented to compare the cost for varying levels of security. When also evaluating risks and benefits, the cost per benefit can be determined for each added level of security. Implementing many levels of security can have a significant impact on the cost consideration for a business or agency, and a value could be assigned to the importance of reliable communications in the operation of various communication services.

8.3 Telephone Wire-tap Capability Implementation

With recent advances in broadband ISDN and ATM switches the FBI has become concerned about maintaining its surveillance wire-tapping capability [25]. Since broadband ISDN and ATM switches are replacing analog switches and current designs contain no standard method of tapping communications, the FBI's 'Digital Telephony Proposal', introduced early in 1993, attempted to mandate the design of standard tapping capabilities into new switches [25]. Apparently the cost of such a re-design was not considered and alternative methods of communication surveillance had not been pursued. Shortly after the 'Digital Telephony Proposal' was introduced it came under fire for infringement of privacy and for infeasibility [3]. Due to the nature of call set-up and control in broadband communications, and ATM in particular, the addition of wire-tapping capability is presently technically infeasible and has no merit in the pursuit of advancing communications capability. Nonetheless, the FBI initially obtained support from the corporate leaders of the major telephone providers and cited the needs of law enforcement agencies. Scenario Three was developed to examine the implementation of the tap capability and the Digital Telephony Model was used to compare the cost of implementation of the tap capability vs. the cost of not implementing the tap capability based on several parameters, including the cost of wire-tapping and the cost of crime.

The major cost factors for implementation of standard wire-tap capabilities are switch design, engineering, and manufacturing costs. Manufacturing costs are in turn based on the number of switches required for telecommunications in the United States. FBI Director William Sessions has estimated the cost would run between $250 and $300 million for telephone switch modifications alone [53]. The major benefit cost

factor is reduction in the amount of crime. For this scenario the reduction in the amount of crime is based on the amount of crime involving digital telephony and pertinent crime statistics. Estimates for this example scenario were obtained through reports on residential and commercial telephone line usage [49,51,53], and reports on crime statistics [4,8,23,24,33,38,45,54,56], including the estimated number of wire-taps, prosecutions, convictions, incarcerations, etc. for various classes of crime. The primary cost factors and values are shown in Table 5. An estimate is used for the research and design cost based upon similar costs for the design of communications equipment. Labor costs for utilization and maintenance of the wire-tap capability are negligible based upon the fact that maintaining present capabilities is desired and no additional personnel will be required. Risks include the possibility of unauthorized eavesdropping or unauthorized disclosure of keys and/or communications. The primary benefit of digital telephony wire-taps is the prevention of crime. This is estimated using figures for the cost of crime [4,8,23,24,33,38,45,54,56], estimating the percent of crimes involving digital telephony, and estimating the percent of those crimes deterred by law enforcement utilization of wire-taps.

A second approach to the implementation of digital telephony wire-taps is implementation on a site-by-site basis as the need arises for law enforcement or national security purposes. In this model the implementation of digital telephony wire-taps apriori (originally designed into equipment) is considered as one side of the issue (Side One), while implementation aposteriori (on a site-by-site basis) is considered as another side to the issue (Side Two). The cost of implementation (apriori or aposteriori) vs. the cost of non-implementation is seen by considering the direct costs plus the indirect risk costs vs. the indirect value of the benefits. Additional sources of cost data values for this scenario can be obtained from the Bureau of Justice Statistics [4,23,24,33,45], from the Criminal Justice Institute [54], from Edna McConnell Clark Foundation [56], from an FBI Law Enforcement Bulletin [22], from a NASA/Ames Research Center publication [31], and from "Planning Models for Analytical Evaluation", the Handbook of Criminal Justice Evaluation [8].

As can be seen in Table 5, the direct costs associated with an initial installation are $55,980,000, while those associated with a retrofit of equipment are $25,500,000. The indirect cost associated with the risks of an initial installation are $11,000,000, and those associated with a delayed installation are $1,100,000. The sum of the direct costs plus risks for implementation of telephone wire-taps apriori is $66,980,000, while the cost of non-implementation (benefits of implementation

TABLE 5: TELEPHONE WIRE-TAP CAPABILITY IMPLEMENTATION MODEL

Side One: Initial Switch Design with Tap Capability (Implementation Apriori)					
Side One Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation (Apriori)	No. of Switches in US	integer		10,000	
	Added Cost per Switch	dollars/switch		25,000	
	Total Cost for Switches	dollars	No. of Switches in US*Added Cost per Switch	250,000,000	
	Total Cost Amortized Over 5 yrs.-Est	dollars/5 yrs	Total Cost for Switches * (1+ 0.1)	275,000,000	
	Total Cost per Year	dollars/yr	Total Cost Amortized Over 5 yrs./5	55,000,000	55,000,000
	One-TimeSwitch Design/Dev. Cost/Vendor	dollars/vender		80,000	
	No. of Vendors	integer		6	
	Total One-Time Design/Dev. Cost	dollars	One-Time Design/Dev. Cost/Vendor* No. of Vendors	480,000	55,480,000
Manage & Operate (Apriori)	Added Staff Years/Switch	years		0	
	Average Loaded Labor Hour	dollars/yr/ switch		75,000	
	Total Operating Cost	dollars	Average Loaded Labor Hour* Added Staff Years/Switch* No. of Switches in US	0	55,480,000
Utilization (Apriori)	Investigation	dollars		0	55,480,000
	Acquisition of Evidence	dollars		500,000	55,980,000
	Prosecution	dollars		0	55,980,000
	Incarceration	dollars/yr		0	55,980,000
System Affected by Tap Capability:					

Public Mail Systems	No. of Telephone Company Switches	integer		6	
	No. of Users per Tel. Company	integer		1,000,000	
	Total Number of Users	integer	No. of Telephone Company Switches*No. of Users/Tel. Company	6,000,000	
Telephone Switches	No. of Residential Telephone Subscribers	integer		260,000,000	
	Percent Using Digital Switches	percent		0.9	
	No. of Residential Subscribers Using Digital Switches	integer	No. of Residential Telephone Subscribers*% Using Digital Switches	26,000,000	
	Cost per Digital Switch	dollars/switch		0	
	Total Cost for Res. Switches	dollars	No. of Residential Subscribers Using Digital Switches*Cost per Dig. Switch	0	
	No. Business Subscribers	integer		10,000,000	
	Percent with PBX Switches	percent		0.75	
	No. of Business Subscribers with PBX Switches	integer	No. Business Subscribers*% with PBX Switches	7,500,000	
	Cost per PBX Switch	dollars/ switch		0	
	Total Cost of PBX Switches	dollars	No. of Business Subscribers with PBX Switches*Cost per PBX Switch	0	
Online Information Software	No. Users Effected	integer		5,000,000	
	Cost per User	dollars/user		0	
	Total Cost for Users	dollars	No. Users Effected*Cost per User	0	
LANs, MANs, and WANs	No. of Networks to be Modified	integer		1,500,000	

	Cost per Network	dollars/ network		0	
	Total Cost for Networks	dollars	No. of Networks to be Modified* Cost per Net.	0	
Radio & Cellular Based Comm Systems	No. of Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
BBS Systems	No. Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Satellite Uplink/ Downlink Equipment	No. of Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Aviation Comm Systems	No. Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Side One Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Risks of Design-ing in Security Taps (Apriori):					
Misuse of Tap Capability (Tel. Company Employees)	Percent of Switches Misused	percent		0.001	
	Cost per Misuse	dollars/ incident		1,000,000	

	Total Cost of Misuse	dollars	No. of Switches in US*% of Switches Misused*Cost per Misuse	10,000,000	65,980,000
Misuse of Info Acquired Legally	Damage/ Invasion of Privacy	dollars		0	
Compromise of Right to Privacy	Subjective Assessment	dollars		0	
Tap Capability Negated or Avoided	Cost of Crimes Avoiding Tap	dollars		1,000,000	66,980,000
Side One Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation (Apriori):					
Courts/Police Costs	Est. Judicial Expenses(1981)	dollars/hour		100	
		hours/day		8	
		days/year		250	
		dollars	Est. Judicial Expenses per hour*(hours/ day)*(days/ year)	200,000	
	Police Costs (1984)	dollars/year		20,000,000	
Prison Costs	Average Cost of Institutional Bed (1982)	dollars/year		50,000	
	Average Cost of Maximum Security Bed (1982)	dollars/year		1,000,000	
	No. of Corrections Employees (1982)	integer		0	
	Cost for Corrections Facilities(1982)	dollars/year		10,000,000,000	
Cost of Crimes	Value of Human Life (Depen- dants' Support)	dollars		0	
	Value of Human Life (Loss of Loved One)	dollars		0	

	Value of Recoverable Property	dollars		0	
	Value of Confiscatable Property/Cash	dollars		0	
	Cost to Society	dollars		0	
Cost of Crimes Involving Digital Telephony:					
Bribery	Value of Bribes Paid/Recovered/Fines	dollars		0	
Burglaries	Number Reported in 1983	integer		5,300,000	
	Value of Losses	dollars		4,000,000,000	
Drug Smuggling/ Sale	Cost of Addiction Programs (Direct)	dollars		10,000,000	
	Cost of Addiction Programs (Indirect)	dollars		0	
	Recovery/Confiscation Value of Property/ Cash	dollars		0	
Extortion	Recovery of Value from Extortion	dollars		0	
Insider Trading	Value of Illegal Gains Recovered/Fines	dollars		0	
Murder	Estimated Cost in 1984	dollars		282,000	
	Value of Human Life (Dependants' Support)	dollars		0	
	Value of Human Life (Loss of Loved One)	dollars		0	
Price Fixing	Cost to Society (Direct)	dollars		0	
	Cost to Society (Indirect)	dollars		0	
Rape	Est. Cost without Bodily Injury (1984)	dollars		24,000	
	Est. Cost with Bodily Injury (1984)	dollars		47,000	

Robbery	Est. Cost of Serious Injury (1983)	dollars		32,000	
	Cost of Property	dollars		500,000,000	
Scandals (S&L, etc.)	Cost to Corporation	dollars		-1,000,000	
	Cost to Taxpayer	dollars		-50,000,000,000	
Terrorist Activity	Destruction of Property	dollars		-50,000,000	
	Destruction of Life	dollars		-50,000,000	
	Cost of Prevention Agencies (US Only)	dollars		-25,000,000	
White Collar Crimes	No. of Cases	cases/year		500	
	Cost per Incident	dollars/case		-100,000	
	Total Cost	dollars	Cost per Incident*No. of Cases	-50,000,000	
Crime Totals	Total Criminal JusticeSpending	dollars		-35,000,000,000	
	Total Cost of Crime	dollars		-85,000,000,000	
	Rise in Crime Cost	factor		1.0	
	Projected Cost of Crime	dollars	Total Cost of Crime*Rise in Crime Cost	-85,000,000,000	
Amount of Telephony Crime	Percent of Crimes Using Dig. Telephony	percent		0.15	
	Cost of Crimes Using Telephony	dollars/year	Projected Cost of Crime*% Using Telephony	-12,768,900,000	
Value of Crimes Prevented	% of Telephony Crime Deterred	percent		0.5	
	Value of Crime Deterred	dollars/year	Cost of Crimes Using Telephony *% Deterred	-6,384,450,000	-6,317,470,000
Side Two: Retrofit of Tap Capability (Implementation Aposteriori)					
Side Two Cost Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation (Aposteriori)	No. of Switches in US	integer		10,000	

	Percentage of Switches Tapped	percent		0.01	
	No. of Switches Tapped	integer	No. of Switches in US*% of Switches Tapped	100	
	Cost to Modify Each Switch	dollars/switch		250,000	
	Total Switch Modification Cost	dollars	No. of Switches Tapped*Cost to Modify Each Switch	25,000,000	25,000,000
Manage & Operate (Aposteriori)	Added Staff Years/Switch	years		0	
	Average Loaded Labor Hour	dollars/yr/ switch		75,000	
	Total Operating Cost	dollars	Average Loaded Labor Hour* Added Staff Years/Switch* No. of Switches in US	0	25,000,000
Utilization (Aposteriori)	Investigation	dollars		0	25,000,000
	Acquisition of Evidence	dollars		500,000	25,500,000
	Prosecution	dollars		0	25,500,000
	Incarceration	dollars/yr		0	25,500,000
System Affected by Tap Capability:					
Public Mail Systems	No. of Telephone Company Switches	integer		6	
	No. of Users per Tel. Company	integer		1,000,000	
	Total Number of Users	integer	No. of Telephone Company Switches*No. of Users/Tel. Company	6,000,000	
Telephone Switches	No. of Residen-tial Telephone Subscribers	integer		260,000,000	
	Percent Using Digital Switches	percent		0.9	

	No. of Residential Subscribers Using Digital Switches	integer	No. of Residential Telephone Subscribers*% Using Digital Switches	26,000,000	
	Cost per Digital Switch	dollars/switch		0	
	Total Cost for Res. Switches	dollars	No. of Residential Subscribers Using Digital Switches*Cost per Dig. Switch	0	
	No. Business Subscribers	integer		10,000,000	
	Percent with PBX Switches	percent		0.75	
	No. of Business Subscribers with PBX Switches	integer	No. Business Subscribers*% with PBX Switches	7,500,000	
	Cost per PBX Switch	dollars/ switch		0	
	Total Cost of PBX Switches	dollars	No. of Business Subscribers with PBX Switches*Cost per PBX Switch	0	
Online Information Software	No. Users Effected	integer		5,000,000	
	Cost per User	dollars/user		0	
	Total Cost for Users	dollars	No. Users Effected*Cost per User	0	
LANs, MANs, and WANs	No. of Networks to be Modified	integer		1,500,000	
	Cost per Network	dollars/ network		0	
	Total Cost for Networks	dollars	No. of Networks to be Modified* Cost per Net.	0	
Radio & Cellular Based Comm Systems	No. of Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
BBS Systems	No. Systems to be Modified	integer		0	

	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Satellite Uplink/ Downlink Equipment	No. of Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Aviation Comm Systems	No. Systems to be Modified	integer		0	
	Cost per System	dollars/ system		0	
	Total Cost for Systems	dollars	No. of Systems to be Modified* Cost per System	0	
Side Two Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Risks of Design-ing in Security Taps (Aposteriori)					
Misuse of Tap Capability (Tel. Company Employees)	Percent of Switches Misused	percent		0.001	
	Cost per Misuse	dollars/ incident		1,000,000	
	Total Cost of Misuse	dollars	No. of Switches in US*% of Switches Misused*Cost per Misuse	100,000	25,600,000
Misuse of Info. Acquired Legally	Damage/ Invasion of Privacy	dollars		0	
Compromise of Right to Privacy	Subjective Assessment	dollars		0	
Tap Capability Negated or Avoided	Cost of Crimes Avoiding Tap	dollars		1,000,000	26,600,000
Side Two Benefit Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Implementation (Aposteriori):					

Courts/Police Costs	Est. Judicial Expenses(1981)	dollars/hour		100	
		hours/day		8	
		days/year		250	
		dollars	Est. Judicial Expenses per hour*(hours/ day)*(days/ year)	200,000	
	Police Costs (1984)	dollars/year		20,000,000	
Prison Costs	Average Cost of Institutional Bed (1982)	dollars/year		50,000	
	Average Cost of Maximum Security Bed (1982)	dollars/year		1,000,000	
	No. of Corrections Employees (1982)	integer		0	
	Cost for Corrections Facilities(1982)	dollars/year		10,000,000,000	
Cost of Crimes	Value of Human Life (Depen-dants' Support)	dollars		0	
	Value of Human Life (Loss of Loved One)	dollars		0	
	Value of Recoverable Property	dollars		0	
	Value of Confiscatable Property/Cash	dollars		0	
	Cost to Society	dollars		0	
Cost of Crimes Involving Digital Telephony:					
Bribery	Value of Bribes Paid/Recov-ered/Fines	dollars		0	
Burglaries	Number Repor-ted in 1983	integer		5,300,000	
	Value of Losses	dollars		4,000,000,000	
Drug Smuggling/ Sale	Cost of Addic-tion Programs (Direct)	dollars		10,000,000	

	Cost of Addiction Programs (Indirect)	dollars		0	
	Recovery/Confiscation Value of Property/ Cash	dollars		0	
Extortion	Recovery of Value from Extortion	dollars		0	
Insider Trading	Value of Illegal Gains Recovered/Fines	dollars		0	
Murder	Estimated Cost in 1984	dollars		282,000	
	Value of Human Life (Dependants' Support)	dollars		0	
	Value of Human Life (Loss of Loved One)	dollars		0	
Price Fixing	Cost to Society (Direct)	dollars		0	
	Cost to Society (Indirect)	dollars		0	
Rape	Est. Cost without Bodily Injury (1984)	dollars		24,000	
	Est. Cost with Bodily Injury (1984)	dollars		47,000	
Robbery	Est. Cost of Serious Injury (1983)	dollars		32,000	
	Cost of Property	dollars		500,000,000	
Scandals (S&L, etc.)	Cost to Corporation	dollars		-1,000,000	
	Cost to Taxpayer	dollars		-50,000,000,000	
Terrorist Activity	Destruction of Property	dollars		-50,000,000	
	Destruction of Life	dollars		-50,000,000	
	Cost of Prevention Agencies (US Only)	dollars		-25,000,000	
White Collar Crimes	No. of Cases	cases/year		500	

	Cost per Incident	dollars/case		-100,000	
	Total Cost	dollars	Cost per Incident*No. of Cases	-50,000,000	
Crime Totals	Total Criminal JusticeSpending	dollars		-35,000,000,000	
	Total Cost of Crime	dollars		-85,000,000,000	
	Rise in Crime Cost	factor		1.0	
	Projected Cost of Crime	dollars	Total Cost of Crime*Rise in Crime Cost	-85,000,000,000	
Amount of Telephony Crime	Percent of Crimes Using Dig. Telephony	percent		0.15	
	Cost of Crimes Using Telephony	dollars/year	Projected Cost of Crime*% Using Telephony	-12,768,900,000	
Value of Crimes Prevented	% of Telephony Crime Deterred	percent		0.5	
	Value of Crime Deterred	dollars/year	Cost of Crimes Using Telephony *% Deterred	-6,384,450,000	
Benefit Not Derived Due to Late Implementation	Percent of Crime Not Deterred	percent		0.02	
Crime Prevented	Value of Crime Deterred (Late Implementation)	dollars/year	Value of Crime Deterred*(1-% of Crime Not Deterred Due to Late)	-6,256,761,000	-6,230,161,000

apriori) is $6,384,450,000. The sum of the direct costs plus risks for implementation of telephone wire-taps aposteriori is $26,600,000, while the cost of non-implementation (benefits of implementation aposteriori) is $6,256,761,000. The sum of direct costs plus risks minus benefits for an initial installation are -$6,317,470,000, while those for a delayed installation are -$6,230,161,000, resulting in a lower cost aposteriori. The cost of implementation apriori is less than any percentage of implementation aposteriori (as shown in Table 6), partly due to the greater design costs for retrofitting this capability. The cost of not implementing broadband communication wire-taps (primarily the cost of crime due to non-implementation) is 9418% greater (or 95 times greater) than the cost of implementing broadband communication wire-taps (apriori). Although the cost of implementation of this initiative is considered significant, the benefit derived from the prevention of crime outweighs the cost.

A parametric analysis was performed to compute the total cost of digital telephony wire-tap implementation aposteriori vs. the percent of switches tapped/retrofitted (as shown in Table 6). As can be seen in Figure 2, the cost increases by 255,000,000 as the percent of switches tapped increases from 0-10%.

Parametric tables were also computed for ranges of the cost of crime (as shown in Table 6), as these values could vary and/or increase greatly due to increasingly more sophisticated criminal activities - and involvement of organizations, companies, and even local government. The parameter used in the Digital Telephony Database to depict the range of crime costs (or increasing cost of crime) is the 'Rise in Crime Cost' factor. This factor is varied from 1 to 10 in steps of 1. Thus, the resulting cost of telephony wire-taps is depicting as the cost of crime doubles, triples, quadruples, etc. The rising cost of crime has been shown to be significant because of increasing crime rates, increasing sophistication, and inflation. Installation of telephony wire-tap capability for digital switches apriori would prevent inflationary costs affecting implementation but not the cost of crime. Therefore, all of these factors affecting the cost of crime are applicable. As can be seen from Figures 3a and 3b, the resulting cost of implementation decreases significantly, since the direct costs are small in proportion to the estimated value of crime deterrence. For this example scenario it is more cost effective to implement wire-tap capabilities apriori, even as the cost of crime increases. The overall cost (direct cost plus risks minus benefits) is linearly dependent on the increasing cost of crime since it is directly proportional.

TELEPHONE WIRE-TAP CAPABILITY IMPLEMENTATION
TABULAR RESULTS

ISSUE 3: IMPLEMENTATION OF TAP CAPABILITY

SIDE 1: Total Cost of Implementation Apriori
SIDE 2: Total Cost of 1% Implem. Aposteriori

SIDE_NUMBE	TOTAL_COST
1	-6,317,470,000
2	-6,230,161,000

SIDE 2: Costs + Risks - Benefits (Aposteriori)
PARAMETER: Percent of Switches Tapped

SIDE_NUMBE	PARAM_VALUE	TOTAL_COST
2	0	-6,255,761,000
	0.005	-6,242,961,000
	0.01	-6,230,161,000
	0.015	-6,217,361,000
	0.02	-6,204,561,000
	0.025	-6,191,761,000
	0.03	-6,178,961,000
	0.035	-6,166,161,000
	0.04	-6,153,361,000
	0.045	-6,140,561,000
	0.05	-6,127,761,000
	0.055	-6,114,961,000
	0.06	-6,102,161,000
	0.065	-6,089,361,000
	0.07	-6,076,561,000
	0.075	-6,063,761,000
	0.08	-6,050,961,000
	0.085	-6,038,161,000
	0.09	-6,025,361,000
	0.095	-6,012,561,000
	0.1	-5,999,761,000

SIDE 1: Costs + Risks - Benefits (Apriori)
PARAMETER: Cost of Crime (Factor)

SIDE_NUMB	PARAM_VAL	TOTAL_COST
1	1	-6,317,470,000
	2	-12,701,920,000
	3	-19,086,370,000
	4	-25,470,820,000
	5	-31,855,270,000
	6	-38,239,720,000
	7	-44,624,170,000
	8	-51,008,620,000
	9	-57,393,070,000
	10	-63,777,520,000

SIDE 2: Costs + Risks - Benefits (Aposteriori)
PARAMETER: Cost of Crime (Factor)

SIDE_NUMB	PARAM_VAL	TOTAL_COST
2	1	-6,230,161,000
	2	-12,486,922,000
	3	-18,743,683,000
	4	-25,000,444,000
	5	-31,257,205,000
	6	-37,513,966,000
	7	-43,770,727,000
	8	-50,027,488,000
	9	-56,284,249,000
	10	-62,541,010,000

Model Results: (1) More Cost-Effective to Implement Tap Capability Apriori;
(2) For Implementation Aposteriori the cost increases by $255,000,000 as the Percent of Switches Tapped Increases from 0-10%
(3) As the Cost of Crime Increases, it is Still More Cost Effective to Implement Tap Capability Apriori

Table 6

RETROFIT OF TELEPHONE WIRE-TAP CAPABILITY - PARAMETRIC ANALYSIS

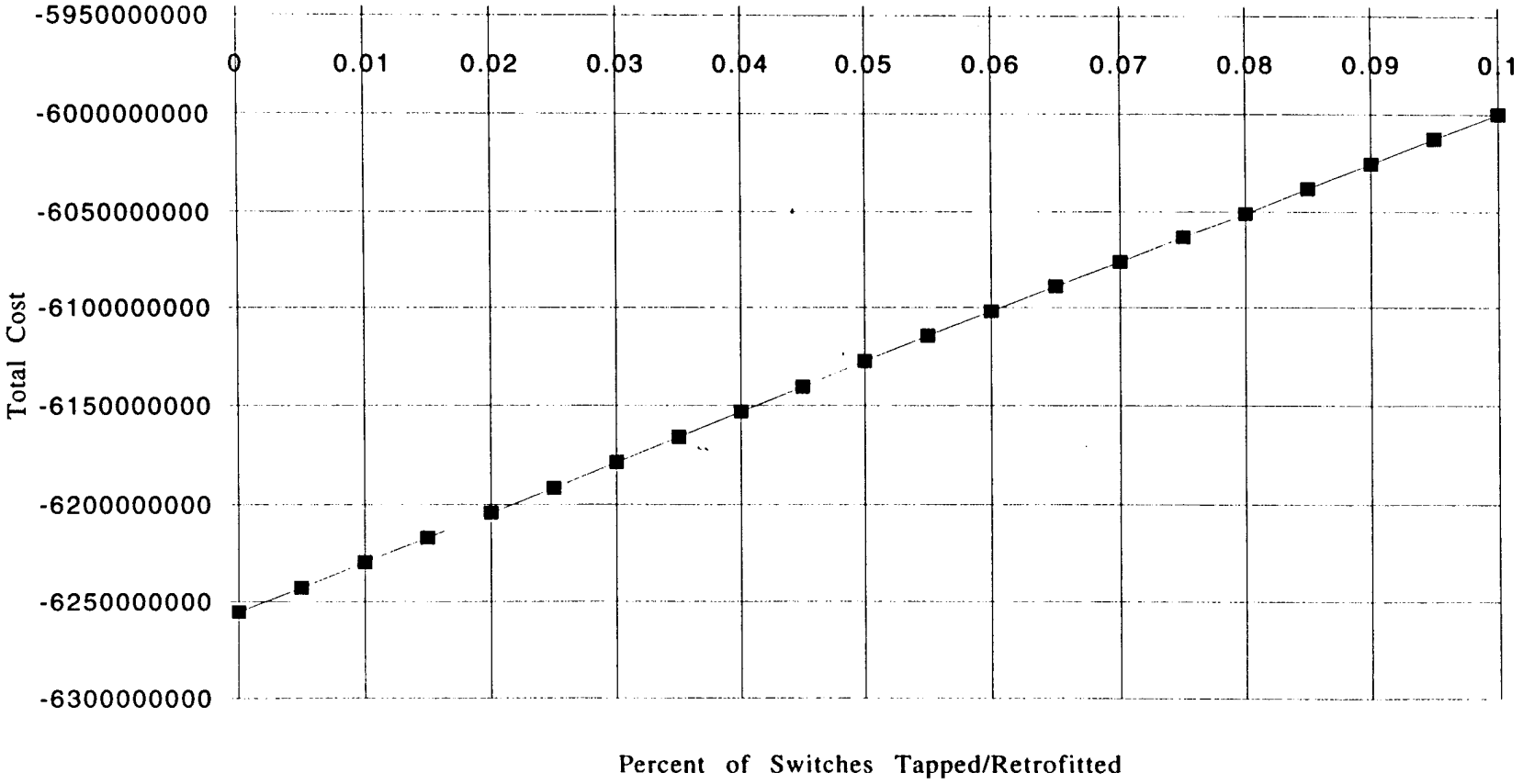


Figure 2

TELEPHONE WIRE-TAP CAPABILITY IMPLEMENTED APRIORI - PARAMETRIC ANALYSIS

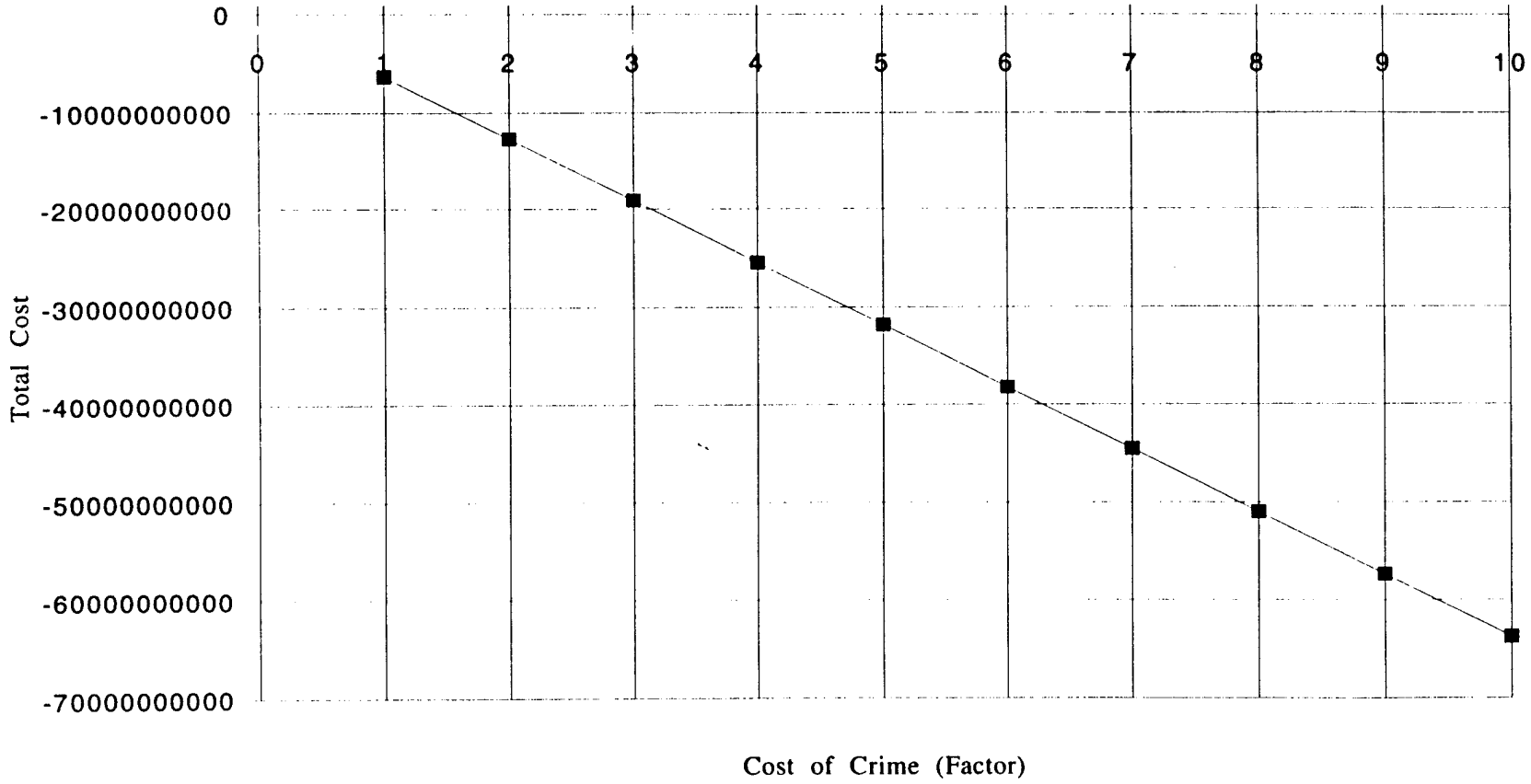


Figure 3a

TELEPHONE WIRE-TAP CAPABILITY IMPLEMENTATION APOSTERIORI PARAMETRIC ANALYSIS

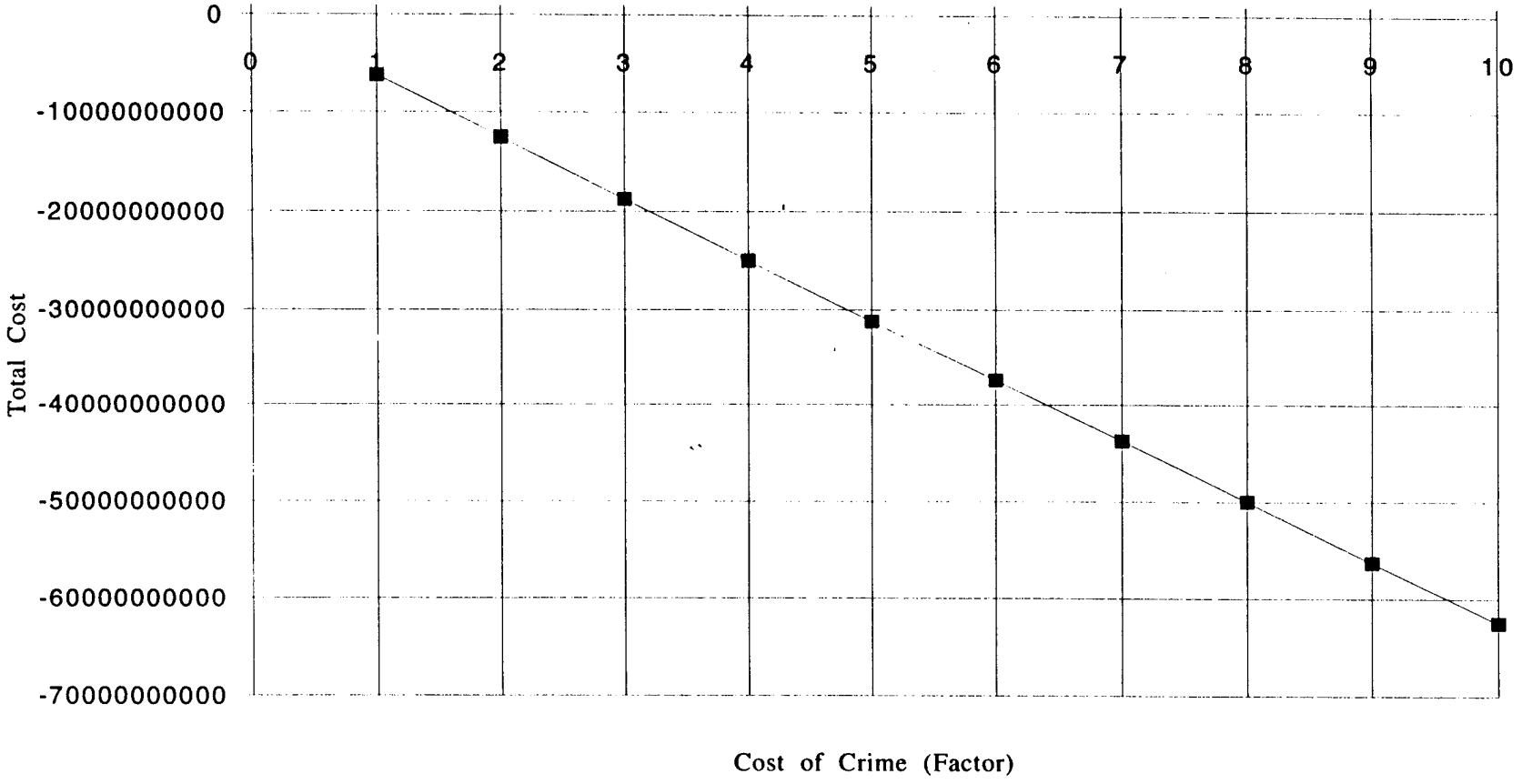


Figure 3b

The model developed for Scenario One (Communication System Implementation Tradeoffs) could be utilized to explore alternatives to the implementation of standard tapping techniques. Consideration of tradeoffs could aid in evaluating the complex technical/engineering design issues and tradeoffs. A lower cost, perfectly viable alternative to implementation of a standard wire-tap capability might exist based on another engineering/technological solution (eg., based on network management techniques).

8.4 Clipper Chip Implementation

When the Clinton administration proposed a hardware encryption chip, the 'Clipper Chip' in the spring of 1994, it was intended for use for all commercial and private communications. Since this would constitute a "monopoly" on cryptographic communication, the software and hardware cryptography industry has strongly opposed any introduction of the Clipper Chip. Even use of the Clipper Chip on a voluntary basis would have a significant impact on the available market in cryptography. One example of this is that AT&T has already announced the inclusion of the Clipper Chip into their new secure telephones [42]. Although there are less costly encryption methods available, many consumers may use the Clipper Chip technology for secure communications for the convenience of being able to buy secure communications "off-the-shelf" as part of a telephone system. In addition, some experts in cryptography and some civil rights groups fear that the Clipper Chip, if implemented widely, might eventually be enforced as the only type of encryption allowed in U.S. communication systems.

Another objection to the Clipper Chip is the inherent registration of keys (key escrow system) and the ability to access communications by law enforcement and national security agencies "as the need for access arises". The algorithm has been designed to use two keys which would be stored in escrow agencies so that law enforcement agencies could decrypt communications when a warrant is obtained. Many experts in the field of cryptography are leery of the Clipper Chip, and of the ability of the Government to secure the keys and prevent unauthorized disclosure of the keys and communication obtained from using the keys. In addition, the algorithm for the Clipper Chip has not been disclosed in its entirety, is classified, and is known only by the Government and a handful of "industry consultants". Since outside access to the algorithm has been denied, the strength of the algorithm has been questioned. An additional issue that does not seem to be addressed anywhere thus far is the need to decipher

both sides of a two-way conversation. The usefulness of deciphering one side of a two-way conversation is questionable. Would this give law enforcement the ability to obtain the keys for anyone called by the party under surveillance? Obviously, many more individuals and organizations would be alarmed at this proposition. The economic considerations in this case would be even more substantial, possibly requiring additional warrants and procedures, and requiring the purchase of additional new phones to ensure future privacy. Also, the risks of unauthorized use would be greater. On the other hand, law enforcement and national security agencies have come to rely on the ability to intercept communications and use the intercepted communications as evidence to convict criminals, monitor compliance to treaties, and guard national security interests. With encryption becoming more widely available, this important surveillance capability is in jeopardy.

At this point the 'Clipper Chip' is slated for use by the Government for all non-classified communications [6,42], and is being implemented by some telephone communication providers [42]. Therefore, the current trend for use of the 'Clipper Chip' is large scale use in Government and commercial communications with other forms of encryption used on a smaller scale. Scenario Four addresses the issues around the 'Clipper Chip' and the costs of implementation to the Government, individuals, and telephone companies, and the cost in possible lost revenues for hardware and software encryption companies. Also included is the cost of crime as might be affected by the Government's inability to decipher communications in a timely manner during investigations because of the use of other encryption products.

In this model Side One represents mandatory use of the Clipper Chip and Side Two represents no implementation of the Clipper Chip. A third possible, and very likely, tradeoff is the voluntary use of the Clipper Chip for private communications. This possibility is labeled as Side Three. In this case the Clipper Chip would not be the only possible means of securing private communications, although with the current support of the Government, the Clipper Chip will probably become the most common means of securing private communications. Considerations for these tradeoffs include the cost of implementation, the benefit derived by national security agencies and law enforcement agencies, and the risk of improper use of key and/or private communication information. The cost of implementation could be broken down to consider the cost to the Government (for design and for implementation for Government use), to telephone companies, and to subscribers. Reliability could be considered with regard to systematically attaining the proper keys for deciphering

communications and also with regard to ensuring keys are only used for official purposes. These would in turn depend upon procedures being properly implemented at several stages of the key escrow system from device manufacturing to key storage to key retrieval. Also, if a single encryption system was mandated, several parties might be interested in finding vulnerabilities in such a system (for instance, criminal defense lawyers, terrorists, drug traffickers, foreign governments, ammunitions (including nuclear) sellers, etc.). Possible subjective parameters are included in the 'Digital Telephony' database (e.g., compromise of right to privacy). These subjective parameters were not assigned values in the examples shown herein, but in exercising the model, one could assign comparative values to subjective parameters on various sides of an issue. Additional considerations are the ability of national security agencies and law enforcement agencies to bring criminals to justice, to interdict drug traffickers, to prevent terrorism, and to control the spread of nuclear technology.

The primary cost factors and values: cost of initial manufacturing and installation, and cost of the key escrow establishment and maintenance are shown in Table 7, along with other cost factors. Maintenance costs include labor hours for maintaining communication equipment and key storage facilities. As can be seen in Table 7, the direct costs associated with mandatory use of the Clipper Chip are $9,139,359,000, while the cost of non-implementation (benefits of implementation) is $13,864,384,462.50. This is based on the number of phones currently in use replaced by 'Clipper Chip' phones and on 90% of targets using the Clipper Chip, and only the Clipper Chip, for encryption. The direct costs associated with voluntary use of the Clipper Chip are $8,229,359,000, and the value of the benefits of implementation based on voluntary usage is $3,080,974,325. This is based on 90% of phones replaced with 'Clipper Chip' phones and 20% of targets using the Clipper Chip, and only the Clipper Chip, for encryption. Of course, the indirect costs associated with potential risks are highly dependent, and therefore, are not modeled here. The sum of direct costs minus benefits for mandatory Clipper Chip usage are -$4,725,025,500, while those for voluntary use of the Clipper Chip are $5,148,384,700, as shown in Table 8. The cost of implementation of the Clipper Chip is 270% greater (or 2.7 times greater) than the cost for non-implementation based on voluntary usage and the cost of voluntary usage is 2.1 times greater than mandated use. The cost of implementation on a voluntary basis is greater than mandated use of the Clipper Chip since the total benefit as seen by law enforcement and national security agencies is not derived. The efficiency of the tools available to law enforcement agencies effects the price paid by American taxpayers both for law

enforcement costs and for the cost of crime. Often, the methods used by law enforcement agencies are necessarily very costly. Therefore, the cost of preventing crime, enforcing justice, and convicting criminals can have a tremendous impact on issues concerned with the ability of law enforcement agencies to effectively enforce the law.

The benefit (to national and law enforcement agencies) of implementation of the Clipper Chip based on voluntary use depends on the percent of individuals/organizations using the Clipper Chip (and no other form of encryption) in cases where a warrant is obtained. Many question the usefulness of the Clipper Chip to law enforcement if other encryption methods are available. Obviously, the percentage of cases using Clipper Chip encryption, and only Clipper Chip encryption, is an unknown parameter at this point. Therefore, in examining the tradeoffs for the Clipper Chip implementation, a parametric analysis was perform by varying this percentage from 0% to 100%. The results of this analysis can be seen in Figure 4 (based on 90% implementation). In this particular implementation, if only the Clipper Chip was used for encryption in 54% of the cases a warrant was obtained, the cost of implementation would be justified. (As can be seen in Table 8 and Figure 4, the cost benefits outweigh the implementation costs at approximately 54%.) One might also consider in this type of analysis that conviction based in part on decrypted Clipper Chip communications would lead to greater use of other encryption devices by "criminals at large".

TABLE 7: CLIPPER CHIP IMPLEMENTATION MODEL

Side One: Implementation of the Clipper Chip					
Side One Cost Element	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Affected Equipment	No. of U.S. Phones	integer		260,000,000	
	Cost per Chip (lots of 10000)	dollars/chip		30	
	Total Chip Cost	dollars	No. of U.S. Phones*Cost per Chip	7,800,000,000	7,800,000,000
	One Time Design Integration Cost	dollars		10,000	7,800,010,000
	Integration Cost per Phone	dollars/phone		5	

	Total Cost for Phone Integration	dollars	No. of U.S. Phones* Integration Cost per Phone	1,300,000,000	9,100,010,000
	No. of Wiretap Installations (1990)	integer		872	
	Average Cost per Installation (Est. 1990)	dollars/ installation		45,125	
	Total Cost of Wiretaps (Est. 1990)	dollars	No. of Wiretap Installations* Average Cost per Installation	39,349,000	9,139,359,000
Side One Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Wiretap Statistics	No. of Resulting Arrests (1990)	integer		2,057	
	No. of Resulting Arrests from 1989	integer		1,486	
	Percent of Arrests Leading to Conviction	percent		0.55	
Clipper Chip Benefit	Percent of Targets Using Clipper Chip	percent		0.9	
	No. of Convictions Resulting w/Clipper Chip	integer	No. of Resulting Arrests*% of Arrests Leading to Conviction* % of Targets Using Clipper Chip	1,753.785	
	Total Non-Traffic Arrests	integer		11,000,000	
	No. of Convictions From Wiretaps	integer	% of Arrests Leading to Conviction * Total Non-Traffic Arrests	6,050,000	
	Total Cost of Crime	dollars		28,000,000,000	
	Total Cost of Crime Involving Wiretaps	dollars	Total Cost of Crime*Percent of Arrests From Wiretaps	15,400,000,000	

	Total Cost of Crime Involving Clipper Chip	dollars	Total Cost of Crime Involving Wiretaps* Percent of Targets Using Clipper Chip	-13,860,000,000	-4,720,641,000
	Value of Crime Prevented per Conviction	dollars/ conviction		2,500	
	Total Deterrence Monetary Benefit	dollars	No. of Resulting Convictions* Value of Crime Prevented per Conviction	-4,384,462.5	-4,725,025,463
Side Two: Non-implementation of the Clipper Chip					
Side Three Cost Element	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Effected Equipment	No. of U.S. Phones	integer		260,000,000	
	Cost per Chip (lots of 10000)	dollars/chip		30	
	Percentage of Phones Using Clipper Chip	percent		0.9	
	Total Chip Cost	dollars	No. of U.S. Phones*Cost per Chip	7,020,000,000	7,020,000,000
	One Time Design Integration Cost	dollars		10,000	7,020,010,000
	Integration Cost per Phone	dollars/phone		5	
	Total Cost for Phone Integration	dollars	No. of U.S. Phones* Integration Cost per Phone	1,170,000,000	8,190,010,000
	No. of Wiretap Installations (1990)	integer		872	
	Average Cost per Installation (Est. 1990)	dollars/ installation		45,125	
	Total Cost of Wiretaps (Est. 1990)	dollars	No. of Wiretap Installations* Average Cost per Installation	39,349,000	8,229,359,000

Side Three Benefit Elem:	Parameters:	Metric:	Formula:	Nom Value:	Totals:
Wiretap Statistics	No. of Resulting Arrests (1990)	integer		2,057	
	No. of Resulting Arrests from 1989	integer		1,486	
	Percent of Arrests Leading to Conviction	percent		0.55	
Clipper Chip Benefit	Percent of Targets Using Clipper Chip	percent		0.2	
	No. of Convictions Resulting w/Clipper Chip	integer	No. of Resulting Arrests*% of Arrests Leading to Conviction* % of Targets Using Clipper Chip	389.73	
	Total Non-Traffic Arrests	integer		11,000,000	
	No. of Convictions From Wiretaps	integer	% of Arrests Leading to Conviction * Total Non-Traffic Arrests	6,050,000	
	Total Cost of Crime	dollars		28,000,000,000	
	Total Cost of Crime Involving Wiretaps	dollars	Total Cost of Crime*Percent of Arrests From Wiretaps	15,400,000,000	
	Total Cost of Crime Involving Clipper Chip	dollars	Total Cost of Crime Involving Wiretaps* Percent of Targets Using Clipper Chip	-3,080,000,000	5,149,359,000
	Value of Crime Prevented per Conviction	dollars/ conviction		2,500	
	Total Deterrence Monetary Benefit	dollars	No. of Resulting Convictions* Value of Crime Prevented per Conviction	-974,325	5,148,384,675

CLIPPER CHIP IMPLEMENTATION
TABULAR RESULTS

ISSUE 4: CLIPPER CHIP IMPLEMENTATION

SIDE 1: Cost of Implementation (Mandatory Use)
(Cost + Risks - Benefits)

SIDE 2: Cost of Non-implementation
(Benefits - Risks)

SIDE 3: Cost of Implementation (Voluntary Use)
(Cost + Risks - Benefits)

SIDE_NUMBER	TOTAL_COST
1	-4,725,025,463
2	13,864,384,463
3	5,148,384,675

SIDE 1: Cost + Risks - Benefits

PARAMETER: Percent of Targets Using Clipper Chip

SIDE_NUMBER	PARAM_VALUE	TOTAL_COST
1	0	8,229,359,000
	0.1	6,688,871,838
	0.2	5,148,384,675
	0.3	3,607,897,513
	0.4	2,067,410,350
	0.5	526,923,187
	0.6	-1,013,563,975
	0.7	-2,554,051,138
	0.8	-4,094,538,300
	0.9	-5,635,025,463
	1	-7,175,512,625

Model Results: For Clipper Chip Implementation to be Worthwhile Approximately 54% of Communications Tapped Must Use the Clipper Chip.

Table 8

CLIPPER CHIP IMPLEMENTATION - PARAMETRIC ANALYSIS

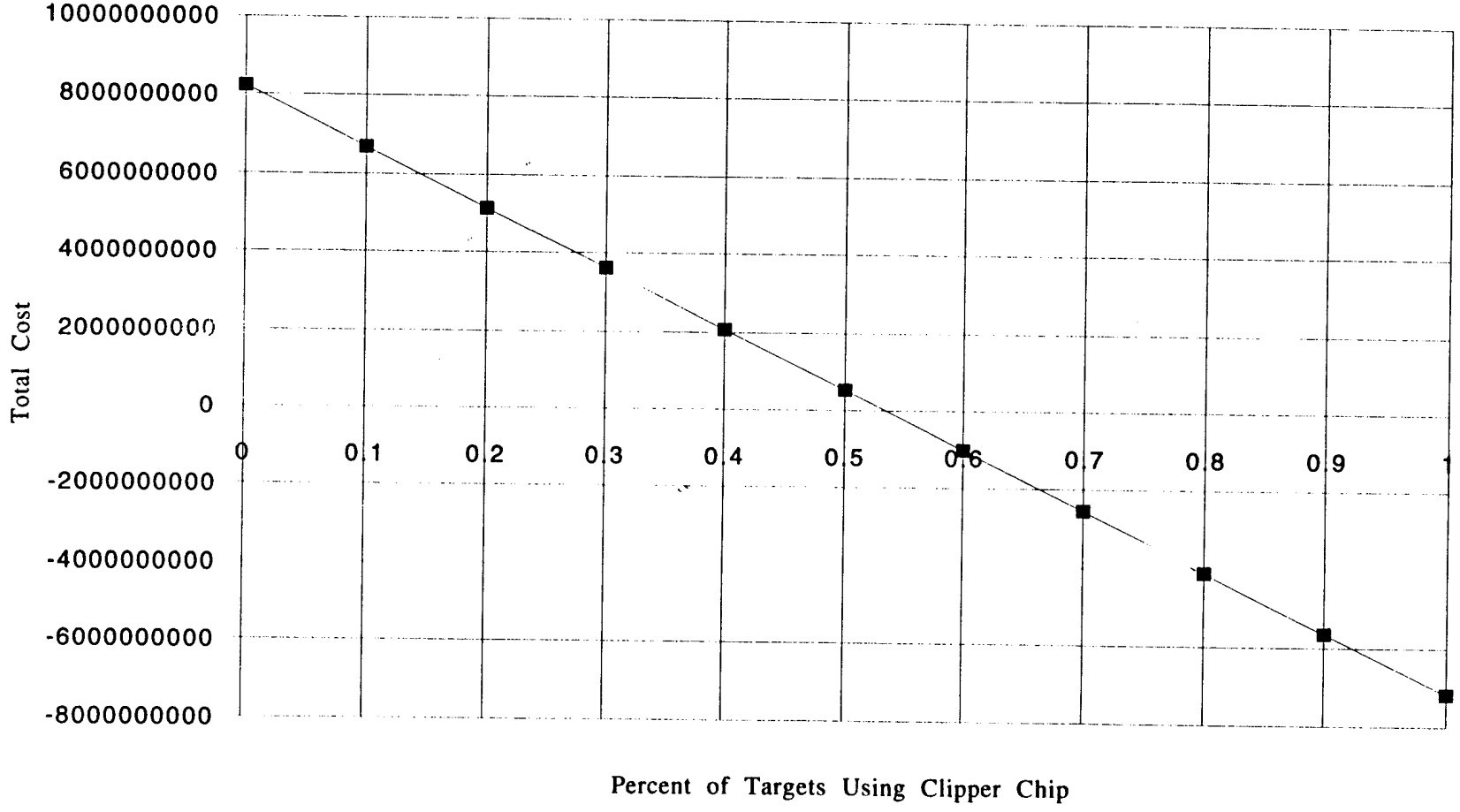


Figure 4

8.5 Registration of Keys vs. Key Privacy

The FBI proposed requiring the registration of all keys used for encryption and decryption of communications in their 'Digital Telephony' proposal [25]. The use of encryption and decryption is becoming more prevalent [21], especially with the introduction of Pretty Good Privacy (PGP) [61], Privacy Enhanced Mail (PEM) [15,36,47,60], and other popular computer utilities [11]. Registration of keys would allow the law enforcement agencies to obtain warrants to obtain registered keys, when authorized, for investigations. Individuals with improperly registered keys would be fined. Of course, the question arises, why would those intending to perpetrate organized crime bother to properly register their keys? A much less severe penalty might result from improperly registered keys than that from a conviction connected to organized crime. Clearly, the benefit of requiring properly registered keys would be directly related to the percentage of keys properly registered in cases where a warrant had been obtained. For example, if all keys had been properly registered for all cases in which warrants had been obtained, then this proposal would be clearly beneficial for law enforcement agencies. On the other hand, if none of the keys had been properly registered for the cases in which warrants had been obtained, then the cost of such a proposal would surely outweigh any benefit obtained by imposing fines for improperly registered keys. Obviously, the costs, risks, and benefits of such a proposal are quite complex with many interdependent factors. Scenario Five addresses a probabilistic scenario given the proposed legislation without additional modification. (Lawmakers could find innumerous variations on methods of implementing such a proposal.)

One issue that does not seem to be addressed anywhere thus far is the need to decipher both sides of a two-way conversation. As more and more individuals and companies use encryption/decryption algorithms, the number of encryption keys involved for the surveillance of all conversations to and from one location tends to grow. Typically, general purpose encryption/decryption algorithms use a public key for encipherment and a private key for decipherment. The public encipherment key is made available to the public so that any communication sent to that recipient could be enciphered with that person's public key. Only the private key can decipher the communication, so that only the intended recipient can convert the message back to plain text. Therefore, in order to monitor outgoing communications from the place of surveillance, the private keys for all recipients would be required. The usefulness of

deciphering one side of a two-way conversation is questionable. Would this give law enforcement the ability to obtain the keys for anyone called by the party under surveillance? Obviously, many more individuals and organizations would be alarmed at this proposition. The economic considerations in this case would be even more substantial, possibly requiring additional warrants and procedures, and requiring the purchase of additional new phones to ensure future privacy. Also, the risks of unauthorized use would be greater. The economic risks and benefits of implementing each side of the issue was computed based on identified contributing factors. Economic benefit is defined in regard to overall national economic benefit, including such parameters as the cost of crime, and the cost of law enforcement and investigations.

This model considers the cost of the registration of private keys, the cost of enforcing private key registration, and the benefits gained by Government in having private keys registered. Side One represents the mandatory registration of keys and Side Two represents no required registration of keys. Registration of keys would require the establishment of procedures and practices for the registration, storage, and retrieval of keys and their associated algorithms, as well as fines for improperly registered keys and/or algorithms. This would require personnel, storage equipment/media, and maintenance of records. This cost would have to be weighed against the benefits. The primary benefit of mandating key registration would be to aid in law enforcement. A secondary benefit might be to deter criminals from committing crimes. In order to assign a value to this benefit one could consider the cost of crime and the possible reduction in that cost by using key registration instead of other surveillance techniques and the possible reduction in the cost of crime by deterrence. Additional considerations are the ability of national security agencies and law enforcement agencies to interdict drug traffickers, to prevent terrorism, and to control the spread of nuclear technology. Risks of implementing mandatory key registration could include the misuse/unauthorized use of key and private communication information by law enforcement agencies, or possibly by telephone company employees. This could results in unauthorized eavesdropping or unauthorized disclosure of keys and/or communications. As more and more services are offered over the network, the affected communications could contain private records such as personal medical information, tax records, assets, as well as corporate records such as banking transactions and proprietary information.

The primary cost factors and values: cost of facilities, equipment, the key registration process, and key storage system maintenance are

shown in Table 9, along with other cost factors. As can be seen in Table 9, the direct costs associated with the registration of keys are $3,014,000. The indirect cost associated with the risks of the registration of keys are $620. The indirect cost associated with the benefits of the registration of keys are -$7,702,435,812.50. The sum of the direct costs plus the indirect costs due to risks minus the indirect costs due to benefits is $7,699,401,192 (as shown in Table 10). The cost of not implementing registration of keys is 2,538% greater (or 25.4 times greater) than implementation, due primarily to the costs of crime prevention and enforcement based on 50% of cases using strong encryption with properly registered keys.

The percentage of cases using strong encryption with properly registered keys is highly variable and constantly changing as more individuals and corporations start to use strong encryption and as the number of those who would properly register their keys is an unknown factor. Therefore, a parametric analysis was performed varying the percentage of cases in which legal intercept warrants were obtained for communications with properly registered keys. This factor was varied from 0-100%. The results of this analysis are shown in Table 10 and Figure 5. For Scenario Five, if the percentage of cases with properly registered keys is at least 0.02%, the benefits of key registration outweigh the direct and indirect costs. As more and more communications are secured with strong encryption, the value of a key registration system becomes more and more valuable to law enforcement and national security agencies. As the use of strong encryption devices approaches 100%, the surveillance capabilities of law enforcement and national security agencies is severely affected by access to encryption/decryption keys and their associated algorithms.

TABLE 9: REGISTRATION OF KEYS MODEL

Side One: Implementation of Key Registration					
Cost Element	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Computing/ Storage Facilities	Cost of Equipment (Annual Basis)	dollars/year		1,500,000	1,500,000
Facility Maintenance	Cost of Maintenance	dollars/year		120,000	1,620,000
Cost of Registration	Labor Costs	dollars/year		1,200,000	2,820,000
Overhead	Cost of Facilities	dollars/year		24,000	2,844,000

	Cost of Management	dollars/year		170,000	3,014,000
Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Unauthorized Access Resulting In:					
Invasion of Privacy	Probability of Occurrence	percent		0.000001	
	Cost of Occurrence	dollars/ occurrence		0	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	0	3,034,000
Bribery	Probability of Occurrence	percent		0.0001	
	Cost of Occurrence	dollars/ occurrence		2,000,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	200	3,034,200
Extortion	Probability of Occurrence	percent		0.0001	
	Cost of Occurrence	dollars/ occurrence		2,000,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	200	3,034,400
Loss of Trade Secrets	Probability of Occurrence	percent		0.00001	
	Cost of Occurrence	dollars/ occurrence		10,000,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	100	3,034,500
Defamation of Character	Probability of Occurrence	percent		0.000001	
	Cost of Occurrence	dollars/ occurrence		50,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	0.05	3,034,500.05
Scandal	Probability of Occurrence	percent		0.00001	
	Cost of Occurrence	dollars/ occurrence		5,000,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	50	3,034,550.05
Insider Trading	Probability of Occurrence	percent		0.00001	

	Cost of Occurrence	dollars/ occurrence		7,000,000	
	Probable Cost	dollars	Probability of Occurrence*Cost of Occurrence	70	3,034,620.05
Side Two: Non-implementation of Key Registration					
Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Wiretap Statistics	No. of Resulting Arrests (1990)	integer		2,057	
	No. of Resulting Arrests from 1989	integer		1,486	
	Percent of Arrests Leading to Conviction	percent		0.55	
Key Registration Benefit	Percent of Targets w/Keys Properly Registered	percent		0.5	
	No. of Resulting Convictions	integer	No. of Resulting Arrests*% of Arrests Leading to Conviction* % of Targets w/Keys Properly Registered	974.325	
	Total Non-Traffic Arrests	integer		11,000,000	
	Percent of Arrests From Wiretaps	percent		6,050,000	
	Total Cost of Crime	dollars		28,000,000,000	
	Total Cost of Crime Involving Wiretaps	dollars	Total Cost of Crime*Percent of Arrests From Wiretaps	15,400,000,000	
	Total Cost of Crime w/ Registered Keys	dollars	Total Cost of Crime Involving Wiretaps* Percent of Targets w/Keys Properly Registered	-7,700,000,000	-7,696,965,380
	Value of Crime Prevented per Conviction	dollars/ conviction		2500	

REGISTRATION OF KEYS
TABULAR RESULTS

ISSUE 5: REGISTRATION OF KEYS

SIDE 1: Total Cost of Implementation

SIDE 2: Benefits - Risks

SIDE_NUMBER	TOTAL_COST
1	3,014,000
2	7,702,435,192

SIDE 1: Costs + Risks - Benefits

PARAMETER: Percent of Warrants for Lines with Keys Properly Registered

SIDE_NUMBER	PARAM_VALUE	TOTAL_COST
1	0.00	3,014,620
	0.10	-1,537,472,542
	0.20	-3,077,959,705
	0.30	-4,618,446,867
	0.40	-6,158,934,030
	0.50	-7,699,421,192
	0.60	-9,239,908,355
	0.70	-10,780,395,517
	0.80	-12,320,882,680
	0.90	-13,861,369,842
	1.00	-15,401,857,005

Model Result: Benefits Outweigh the Cost and Risks if at Least 0.02% of Tap Warrants are for Lines with Properly Registered Keys.

Table 10

REGISTRATION OF KEYS - PARAMETRIC ANALYSIS

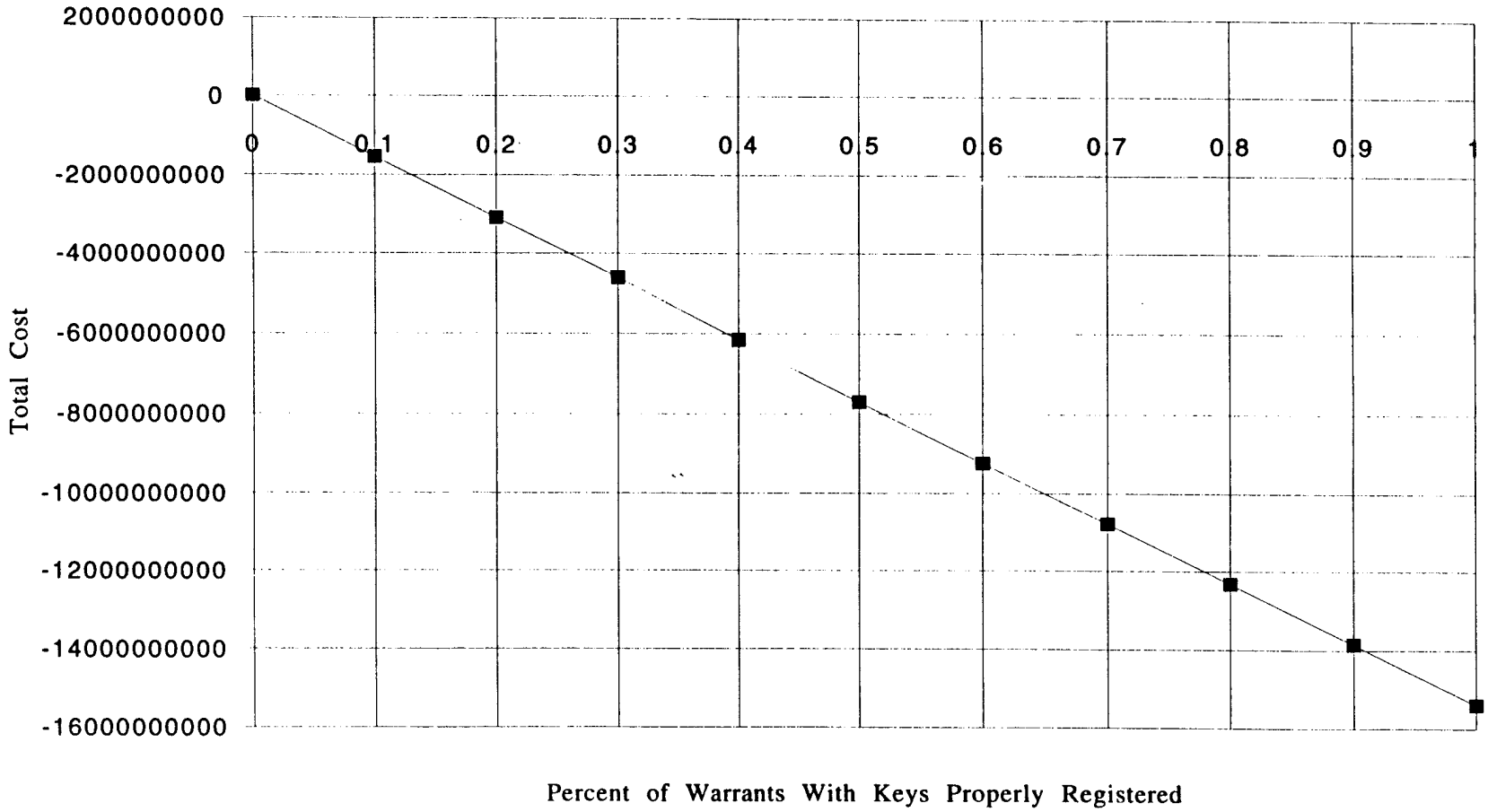


Figure 5

8.6 Export Control of Cryptographic Technology

Export controls on cryptographic devices have been in existence during the Reagan and Bush presidential terms. U.S. export controls on cryptographic devices went into effect in the '70's when the RSA (Rivest, Shamir, and Adelman) algorithm was first restricted from export [34,46]. Since the export restrictions were initiated, several variations of the RSA algorithm have been made available over the Internet [47], yet the export restrictions remain in effect to prevent widespread proliferation and thereby provide some impediment to criminals using strong encryption in places where the U.S. would not be able to obtain keys [30,43]. The removal of these export controls is being discussed [12]. Arguments against export controls state that the technology banned from export is already available outside the U.S. and that better cryptographic systems are being developed outside the U.S. [26]. Therefore, the export controls serve no purpose and actually make it more difficult for the U.S. to compete [13]. At present there is no market per se for cryptographic devices, but the potential for a European cryptographic market appears to be very great. If export controls on cryptographic devices were lifted, the U.S. could potentially control a large share of this potential market. Presently export controls prevent strong encryption from being exported and in this case, U.S. companies would be at an extreme disadvantage if the cryptographic sales "take off". On the other hand, if strong encryption is allowed to be exported with no way for the U.S. Government to decrypt communications (i.e., no "back door"), a number of organized criminal activities may be very difficult to control. Scenario Six was developed to analyze this issue, taking into account several important factors pertinent to national security and to U.S. economic interests.

This model attempts to use relative values to quantitatively determine the tradeoff. The primary tradeoffs are (1) export controls on all strong cryptographic technology, (2) no export controls on cryptographic technology, and (3) limited control on cryptographic technology. The cost of lifting the export restrictions has not been well defined. Factors would involve the cost incurred to national security agencies by the loss of surveillance. This could impact the U.S. in the form of terrorism, drug trafficking, organized crime, and loss of military surveillance. The economic benefit of lifting the ban of export controls is also not well-defined, since the primary benefit, potential U.S. sales oversees, is not established. Since some foreign manufacturers have begun selling encryption devices, the potential for a large cryptographic market seems to exist. Since the impact of several factors is unknown,

parametric analyses can be performed to assist in determining the costs, risks, and benefits of lifting the ban on strong encryption technology exports. A parametric analysis was performed based on the percent of U.S. market share prevented based on a postulated $33,600,000 market in encryption technology oversees in five years.

The primary cost factor, as shown in Table 11, is loss of U.S. export sales. The direct costs associated with export control of cryptographic technology are $21,162,342. The indirect benefit associated with export control of cryptographic technology is determined to be $50,000,000 given the cost of crime parameters, values, and results from Scenario Three. The indirect costs associated with the risks represent a possible erosion of the benefits associated with the availability of foreign encryption products and are $25,000,000. The sum of direct costs and risks minus benefits for continues export control of cryptographic technology are computed to be -$3,837,658. The cost of discontinuing export controls ($50,000,000-$25,000,000) is 18% greater than the projected cost in lost U.S. sales abroad ($21,162,342). The tabular results and conclusions are shown in Table 12.

A parametric analysis was performed varying the probability that strong foreign encryption products are used in cases targeted for surveillance. Of course, strong encryption products obtained outside the U.S. would make surveillance difficult and null the effect of restricting similar exports. As can be seen in Figure 6, if foreign encryption products are used in 58% of the cases, it would economically make sense to lift export controls. Even though encryption is not widely used at present, many anticipate that its use will grow rapidly, in which case it would be advantageous to lift export controls. Since the security of a nation is often tied to the nation's economic well-being, especially today, it is worthwhile to compare the costs of policies with regard to the costs of implementing law enforcement and national security measures.

A parametric analysis was also performed based on varying the percent of the U.S. market share prevented based on current export control laws which restrict only particular encryption/decryption algorithms. As seen in Figure 7, it is more economically feasible to maintain export controls. If most of the U.S. market share is lost, the benefit of maintaining export controls becomes small. A major factor in this analysis is that those seeking to encrypt communications would choose to use the strongest encryption methods available. Since there is not a direct cost increase related to the strength of the encryption method, this would be a plausible assumption. Given this assumption, it is likely that

TABLE 11: EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY MODEL

Side One: Continuance of Export Controls					
Cost Element	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
U.S. Sales of Cryptographic Systems	Target Year	year		5	
	Total Value of Sales Postulated (Internationally)	dollars/year	15,000,000* (Target Year** 1/2) + 10,000 *Target Year	33,591,020	
	U.S. Market Share Postulated	percent		0.70	
	Fraction of U.S. Market Share Prevented	percent		0.90	
	Total Sales Prevented per Year	dollars/year	Total Value of Sales Postulated (Internationally) *U.S. Market Share Postulated*Fraction of U.S. Market SharePrevented	21,162,342	21,162,342
Risk Element:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Benefit Projection Erased By Foreign Products	Probability Strong Encryption Used	percent		0.5	
	Amount of Value Erased	dollars/year	Value of Crimes Affected * Probability Strong Encryption Used	25,000,000	46,162,342
Side Two: Lifting of Export Controls					
Benefit Elem:	**Parameters:**	**Metric:**	**Formula:**	**Nom Value:**	**Totals:**
Crimes Undetectable if U.S. Products Allowed	Value of Crimes Affected	dollars/year		-50,000,000	-3,837,658

EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY
TABULAR RESULTS

ISSUE 6: EXPORT CONTROL OF CRYPTOGRAPHY

SIDE 1: Total Cost (Loss of Sales)

SIDE 2: Benefits - Risks

SIDE	TOTAL_COST
1	21,162,342
2	25,000,000

SIDE 2: Costs + Risks - Benefits

PARAMETER: Probability Strong Encryption Used

	SIDE	PARAM_VALUE	TOTAL_COST
	2	0.00	-28,837,658
1:		0.10	-23,837,658
		0.20	-18,837,658
		0.30	-13,837,658
		0.40	-8,837,658
		0.50	-3,837,658
		0.60	1,162,342
		0.70	6,162,342
		0.80	11,162,342
		0.90	16,162,342
		1.00	21,162,342

SIDE 1: Costs + Risks - Benefits

PARAMETER: Percent of U.S. Market Share Prevented

2:	SIDE	PARAM_VALUE	TOTAL_COST
	1	0.00	-25,000,000
		0.10	-22,648,629
		0.20	-20,297,257
		0.30	-17,945,886
		0.40	-15,594,514
		0.50	-13,243,143
		0.60	-10,891,772
		0.70	-8,540,400
		0.80	-6,189,029
		0.90	-3,837,658
		1.00	-1,486,286

SIDE 1: Postulated Market

PARAMETER: Target Year

	SIDE	PARAM_VALUE	TOTAL_COST
	1	0	0
3:		1	15,010,000
		2	21,233,203
		3	26,010,762
		4	30,040,000
		5	33,591,020
		6	36,802,346
		7	39,756,270
		8	42,506,407
		9	45,090,000
		10	47,534,165
		11	49,859,372
		12	52,081,524
		13	54,213,269
		14	56,264,861
		15	58,244,750
		16	60,160,000
		17	62,016,584
		18	63,819,610
		19	65,573,484
		20	67,282,039

SIDE 1: Costs + Risks - Benefits

PARAMETER: Target Year

4:	SIDE	PARAM_VALUE	TOTAL_COST
	1	0	-25,000,000
		1	-15,543,700
		2	-11,623,082
		3	-8,613,220
		4	-6,074,800
		5	-3,837,658
		6	-1,814,522
		7	46,450
		8	1,779,036
		9	3,406,700
		10	4,946,524
		11	6,411,404
		12	7,811,360
		13	9,154,360
		14	10,446,862
		15	11,694,193
		16	12,900,800
		17	14,070,448
		18	15,206,354
		19	16,311,295
		20	17,387,685

Model Result: (1) The Benefits of Lifting Export Controls Outweigh the Economic Benefits of Maintaining Export Controls if Strong Encryption is Used in At Least 58% of "Targeted" Communications. Therefore, in this Example, it is Better to Maintain Export Controls at the Present Time; However, with the Anticipated Trend Toward Wide Use of Stromg Encryption, Very Shortly the Benefits of Lifting Export Controls May Be Greater.

(2) The Benefits of Export Controls Outweigh the Benefits of Lifting Export Controls at Present and in the Near Future.

(3) The Value of the Global Encryption Market is Expected to Increase Exponentially at First, and then Increase Linearly with Inflation

(4) The Benefits of Lifting Export Controls is Expected to Outweigh the Economic Benefit of Maintaining Export Controls in Approximately 7 Years

Table 12

EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY FOREIGN PRODUCT IMPACT - PARAMETRIC ANALYSIS

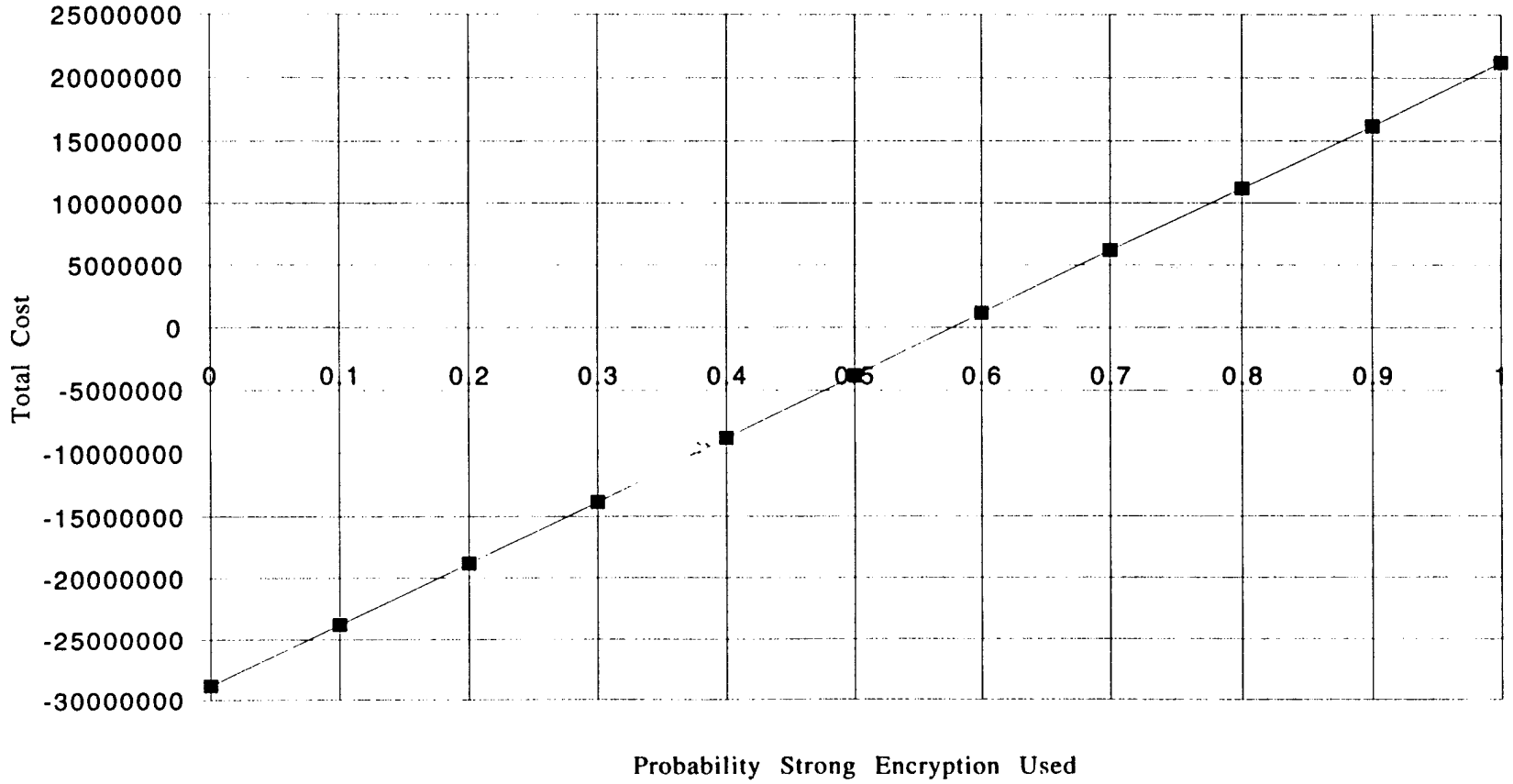


Figure 6

EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY SALES IMPACT - PARAMETRIC ANALYSIS

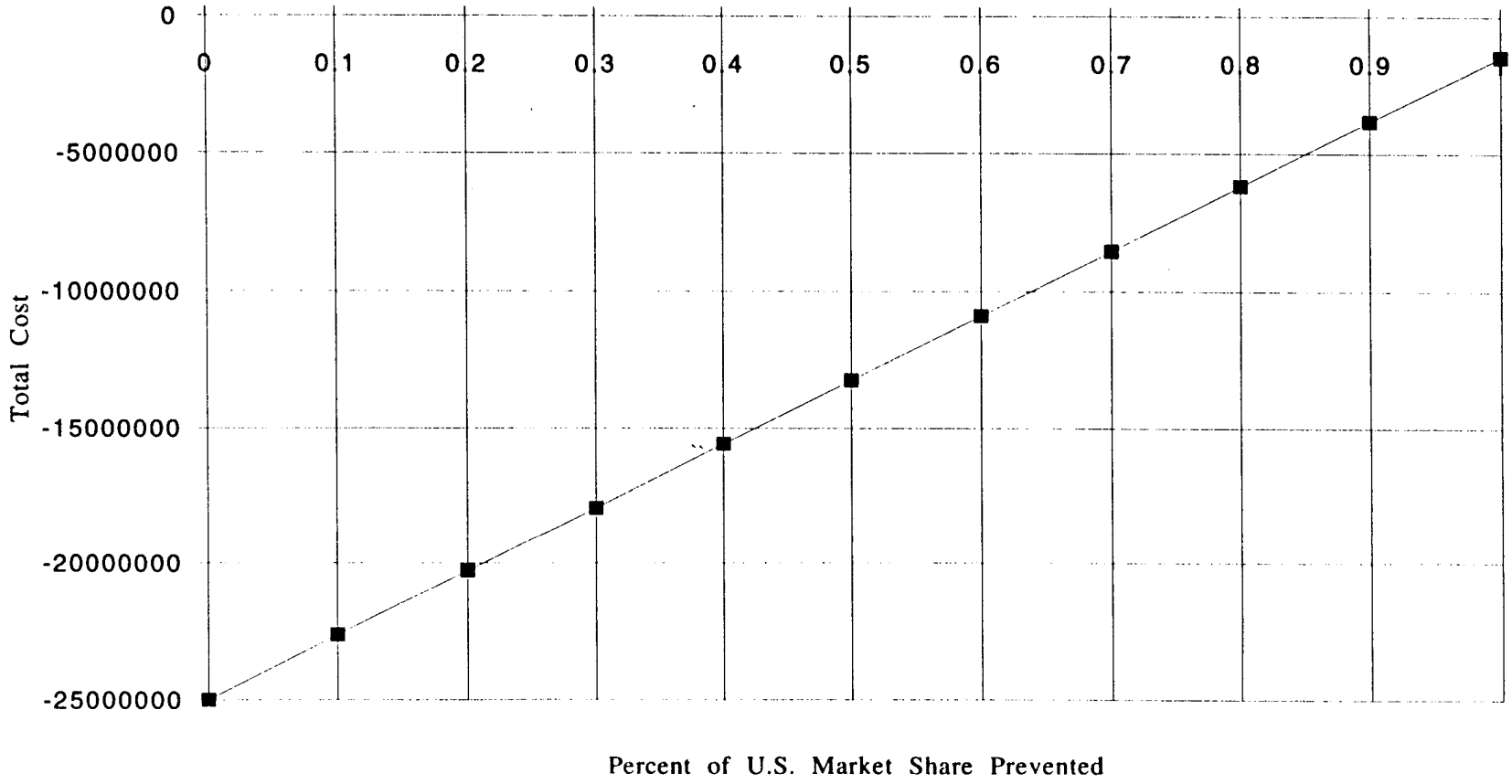


Figure 7

the U.S. cryptographic industry would lose a sizable portion of the available market share.

Current arguments for lifting export controls center on the availability of some export-controlled algorithms overseas. On the other hand, for most consumers the use of encryption depends on the availability of commercial off-the-shelf (COTS) products. One real question is whether foreign manufacturers will make COTS encryption products readily available, and if so, how long will it take to make these products available.

Since the potential value of the cryptographic market oversees is unknown, a parametric analysis was performed based on the assumption that the cryptographic market will grow exponentially at first, and then linearly based on inflation. A hypothetical growth curve is shown in Figure 8. The total cost of maintaining the current export restrictions, based on the postulated growth curve, is displayed in Figure 9. As seen in Table 12, the postulated market is expected to be approximately $47,534,165 in 10 years and approximately $67,282,039 in 20 years. The total cost of continuing the current export restriction policy is postulated to be $4,946,524 and $17,387,685 in 10 and 20 years, respectively. These figures take into account an economic benefit of continuing the current export control policy of approximately $25,000,000 for reduction in crime costs due to export controls.

EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY POSTULATED MARKET - PARAMETRIC ANALYSIS

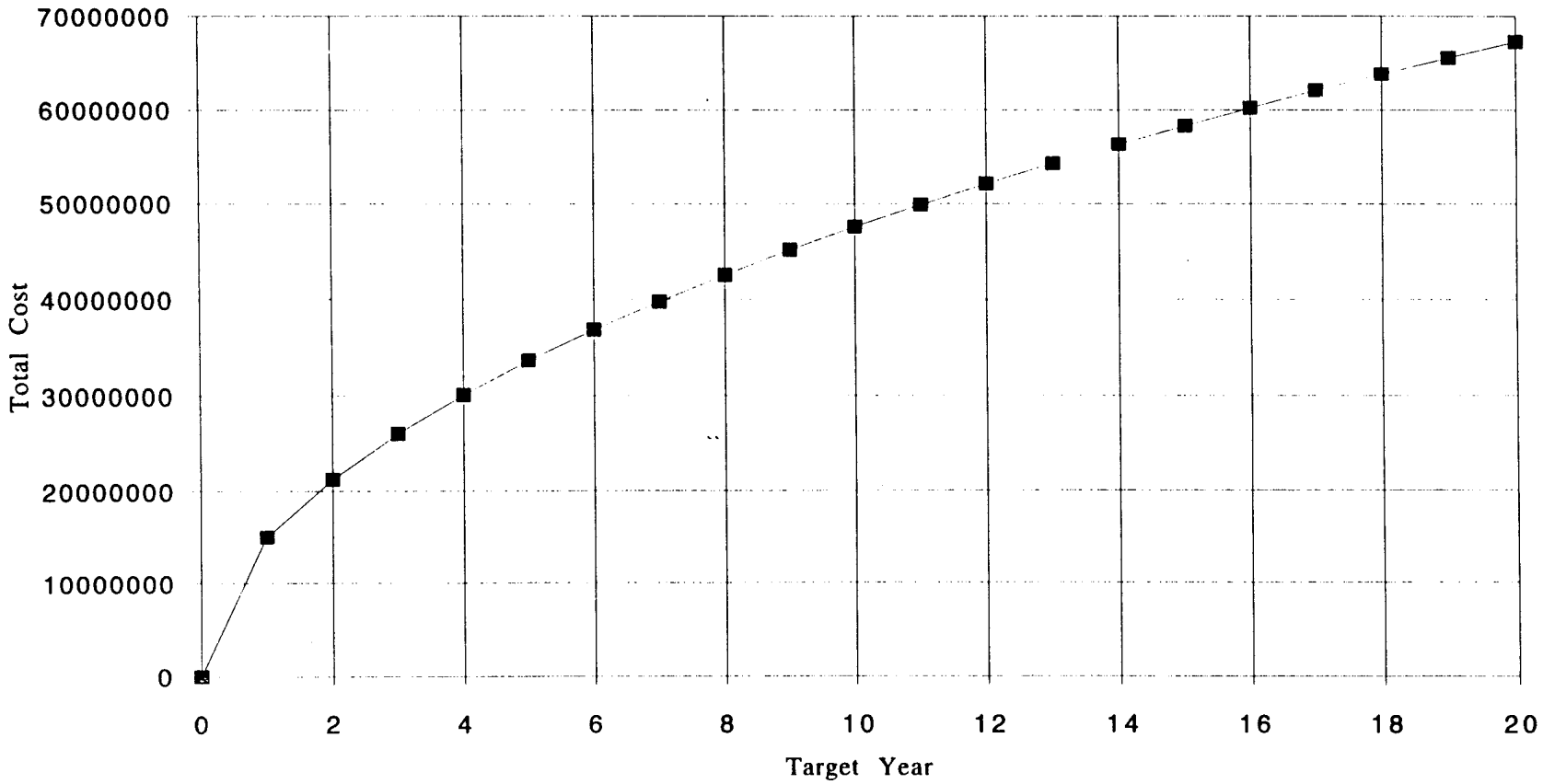


Figure 8

EXPORT CONTROL OF CRYPTOGRAPHIC TECHNOLOGY PROJECTED COST - PARAMETRIC ANALYSIS

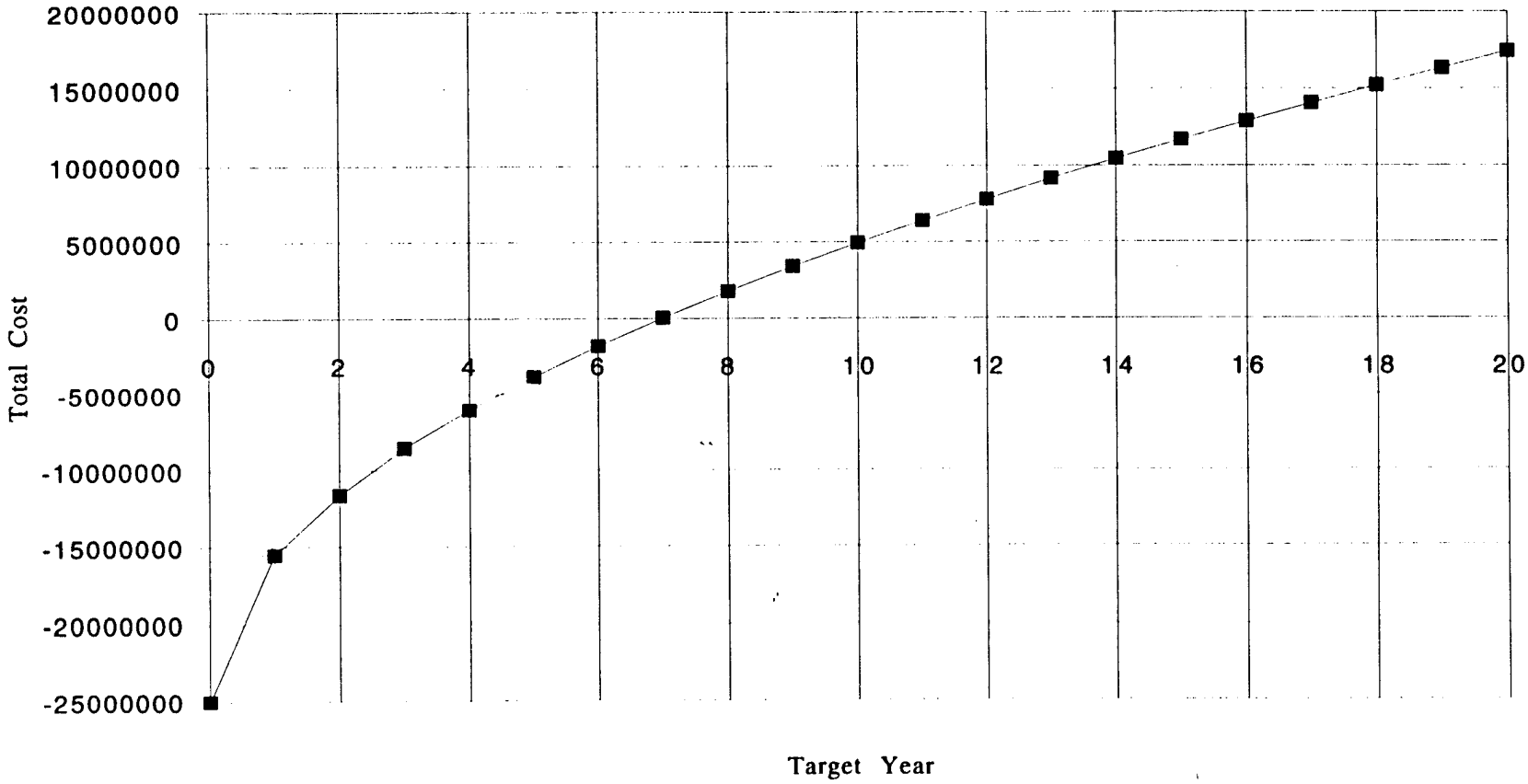


Figure 9

9.0 Conclusion

Several issues are discussed that are relevant to digital telephony and, in particular, to recent advancements in broadband communications. The six issues presented herein are (1) security implementation tradeoffs, (2) initial design with security vs. retrofit, (3) telephone wire-tap capability implementation, (4) 'Clipper Chip' implementation, (5) registration of keys, and (6) export control of cryptographic technology. The issues are developed to the extent required to support the usefulness of the model presented herein to address issues in digital telephony. The summary of the issues is also intended to provide some background to current issues of general public interest and debate. The primary arguments for and against issues are outlined, the primary supporters of different sides of various issues are given. Detailed information on the efforts of individual lobbyists, congressmen, government officials, privacy-rights organizations, and others, as well as the present status of policies can be monitored through news groups [28], the media [11,30,39,41,42,49,53], the Privacy Advisory Board [13], the export control laws [18], information from privacy rights advocates [2,3], communication standards agencies [6,9,16,22,25], and from experts in a particular field [18,19,21,48].

For each of the six issues presented, a scenario was developed to examine some of the possible tradeoffs with regard to the issue. Six scenarios have been developed and described herein, corresponding to the six issues discussed and summarized. The first two scenarios ((1) security implementation tradeoffs, and (2) initial design with security vs. retrofit) deal primarily with issues of interest to individual businesses. The model development and associated parameters for Scenario One can be used to address tradeoffs between various manufacturers, hardware vs. software implementations, various encryption/decryption algorithms, and other security implementation tradeoffs. The model development and associated parameters for Scenario Two can be used to address the financial tradeoffs between initial communication design with security considerations vs. initial non-secure communications design with security retrofitted at a later time. Factors can include financing options, redesign costs, quantity-based discounts, and other pertinent factors.

The remaining four scenarios are developed around current national issues regarding digital telephony (or Integrated Services Digital Network). Scenario Three presents the current tradeoffs and arguments for and against the implementation of telephone wire-tapping capability.

The cost of this implementation would include the cost for redesigning digital switches to provide wiretapping capability similar to their analog counterparts. This is not a straight-forward redesign. The primary benefits are in increasing the effectiveness of law enforcement and national security agencies. Scenario Four is developed around the proposed implementation of the 'Clipper Chip'. The cost of incorporating the 'Clipper Chip' device into communications equipment and registering keys is compared to the benefits obtained by law enforcement and national security agencies. Mandatory and voluntary usage of the 'Clipper Chip' is considered in the analysis. Scenario Five develops a model for analyzing the cost vs. benefits for implementation of key registration for all encryption/decryption devices and their associated algorithms. Again, the implementation costs are compared against the benefits derived by law enforcement and national security agencies. The last scenario is built around the issue of export controls for strong encryption algorithms and devices. The cost (in the form of lost U.S. postulated revenues) is compared to the benefits derived by national intelligence agencies by current export control restrictions.

The basis and factors for the results in each of these executions of the model can be traced to the given parameters, values, and formulas used to calculate total costs as shown in Tables 1, 3, 5, 7, 9, and 11. Non-linear parameters are modeled using non-linear formulas (as shown in Table 11) or using Excel functions (as shown in Table 3). The results displayed in Tables 2, 4, 6, 8, 10, and 12 display the tables generated by the model to display the model results for basic tradeoffs and parametric analyses. All of the corresponding plots (Figures 1-9) were automatically generated by the Parametric Analysis macros.

Note that current and accurate values for data and statistics must be obtained to evaluate any communication tradeoff, whether the tradeoff involves technical or political issues. For the examples given, research on parameters and values was based on figures generally available, [4,5,8,23,24,31,33,38,45,49,51,54,56] requiring that some parameter values be estimated. Normally figures based on statistics are constantly changing, and determining the most realistic value for a cost analysis is difficult. For example, the number of phones in the U.S. is estimated to be 260,000. If the Clipper Chip was implemented, how many of these phones would be replaced? This would be based on the length of time allotted for replacement, advertising campaigns, and changes in population. Several parameters and values have been incorporated into the Digital Telephony database for use with the developed model. The impact of most issues discussed herein is wide-ranging and, therefore, the total impact on

related industries, policies, and procedures is difficult to assess. As a consequence the model is constructed so that additional parameters can easily be incorporated.

The intention in the construction of this model was to provide a generic framework within which any issue in digital telephony could be described on the basis of cost, risks, and benefits. To implement the model each issue and side of an issue is given a numeric label, and a common command macro button is used to run the model, tabulating the cost, risks, and benefits for each side of the indicated issue. An additional command macro button is optional used to calculate parametric tables and plots for ranges of variance for a parameter. Additional parameters can easily be added to the worksheet. Modeled in Excel for portability and immediate use by the large Excel customer base, it is anticipated that this model can be quickly implemented in general for a wide range of cases.

10.0 Acknowledgments

The initial model development and a brief initial report were initially developed by the author for a course in 'Telecommunications Security' at the George Washington University. As such, the author wishes to acknowledge Dr. Lance Hoffman for providing the incentive to develop the baseline model. The author also wishes to acknowledge Mr. David Kohls for providing several of the parameters and values which were included in the digital telephony database. In addition, the author wishes to acknowledge the support and encouragement of Mr. Donald Kallgren to expand the model and compile the model development and results into a formal report.

11.0 References

[1] Acampora, Anthony S., *An Introduction to Broadband Networks*, Plenum Press, New York, 1994

[2] American Civil Liberties Union, "Cryptographic Issue Statements Submitted to the Computer System Security and Privacy Advisory Board", National Institute of Standards, 27 May 1993, pp. 195-9

[3] "An Analysis of the FBI Digital Telephony Proposal", Electronic Frontier Foundation, Washington, D.C., 1992

[4] "A National Assessment of Serious Juvenile Crime", *Reports of the National Juvenile Assessment Centers*, Bureau of Justice Statistics, U.S. Department of Justice, April 1980

[5] Anthes, Gary H., "Use Outpaces Addresses on Internet", *Computer World*, Vol. 27, No. 17, 26 April 1993, pp. 51-2

[6] "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)", National Institute of Standards and Technology, *Federal Register* Vol. 58, No. 145, 30 July 1993, pp. 40791-4

[7] Black, Uyless, *OSI: A Model for Computer Communications Standards*, Prentice Hall, NJ, 1991

[8] Blumstein, A., "Planning Models for Analytical Evaluation", *Handbook of Criminal Justice Evaluation*, Sage Publications, 1981

[9] Brickell, E., et al., "SKIPJACK Review Interim Report: The SKIPJACK Algorithm", National Institute of Standards and Technology, 28 July 1993

[10] Chandler, James, Class Discussions in Telecommunications and Computers, George Washington University, Washington, D.C., 14 April 1993

[11] Chaum, David, "Achieving Electronic Privacy", *Scientific American*, Vol. 267, No.2, August 1992, pp. 96-101

[12] Christensen, L.E., "Technology and Software Controls in Law and Policy of Export Controls: Recent Essays on Key Export Issues", Section of *International Law and Practice of American Bar Association*, August 1993, pp. 3-33

[13] Computer System Security and Privacy Board Resolution, 1-2 September 1993, pp. 93-5

[14] Corcoran, Elizabeth, and Mintz, John, *The Washington Post*, 21 July 1994, Section A, p. 1

[15] Crocker, Stephen, "Internet Privacy Enhanced Mail, *The Third CPSR Cryptography and Privacy Conference Source Book*, 7 June 1993

[16] "Data Encryption Standard", National Bureau of Standards, FIPS PUB 46, January 1977

[17] Datapro, Inc., "Datapro Report on Encryption Devices, Delran, NJ, March 1993

[18] Delaney, D.P., D.E. Denning, J.Kaye, and A.R. McDonald, Risks-Forum Digest, "Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line", Vol. 15: Issue 10, October 8, 1993

[19] Denning, D., *Cryptography and Data Security*, Addison-Wesley, 1982

[20] Denning, D., "To Tap Or Not To Tap?", *Communications of the ACM*, Vol. 36, No. 3, March 1993, pp. 25-44

[21] Diffie, W., and Hellman, M.E., "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22, November 1976, pp. 644-654

[22] "Digital Telephony: Keeping Pace with Technology", *FBI Law Enforcement Bulletin*, August 1992

[23] "Economic Cost of Crime to Victims", *Bureau of Justice Statistics*, U.S. Department of Justice, April 1984

[24] "Economic Impact", *Reports of the National Juvenile Justice*

Assessment Centers, U.S. Department of Justice, April 1980

[25] "FBI Digital Telephony Proposal", Electronic Frontier Foundation, Washington, D.C., 1992

[26] Fischer, Addison, "Cryptographic Issue Statements Submitted to the Computer System Security and Privacy Advisory Board", NIST, 27 May 1993, pp. 204-15

[27] Fisher International, Hewlett-Packard, and Racal-Guardata, Statements before the Computer System Security and Privacy Advisory Board, 29 July 1993

[28] Forum On Risks To The Public In Computers And Related Systems, ACM Committee on Computers and Public Policy, moderated by Peter G. Neumann

[29] Gaffin, Adam, "Internet's In and SNA's Out", Network World, Vol. 11, No. 40, 10 October 1994

[30] Groner, Jonathan, "When It Comes to Software, U.S. Sees Military Hardware; Concern over Spread of Encryption Codes Hurts Exports", *The Connecticut Law Tribune*, 21 December 1992, p. 12

[31] Hanson, Robin, "Would Wiretap Chip Be Cost-Effective?", NASA/Ames Research Center, Information Sciences Division, April 21,1993

[32] Helgert, Hermann J., *Integrated Services Digital Networks*, Addison-Wesley Publishing Company, Inc., 1991

[33] "Households Touched by Crime", Bureau of Justice Statistics, U.S. Department of Justice, May 1984

[34] International Traffic in Arms Regulation (ITAR), 22 CFR, pp. 120-30

[35] Karle, Jerome, Nobel Laureate Presentation, Naval Research Laboratory, 14 June 1993

[36] Kent, Stephen, "Internet Privacy Enhanced Mail",*Communications of the ACM*, Vol. 36, No. 8, 8 August 1993, p.48

[37] Kobielus, James, "Government Should Deregulate Crypto Technologies Market", Network World, 27 June 1994

[38] Lauder, Ronald S., *Fighting Violent Crime in America*, Dodd, Mead, & Company, New York, 1985

[39] Markoff, John, "Thing", *The New York Times*, 5 September 1993, Section 9, p.11

[40] Microsoft Excel 4.0, Designing and Writing a Command Macro, Chapter 7, User's Guide 2

[41] Peterson, Ivars, "Encrypting Controversy", *Science News*, 19 June 1993, pp. 394-396

[42] Press Release Concerning the Key Escrow Initiative, The White House, 16 April 1993

[43] Regan, Edward, "United States Business Views On Encryption and The Key Escrow Chip", Statements before the Computer System Security and Privacy Advisory Board, 30 July 1993

[44] Report No. 782, International Resource Development, Data, Fax, and Voice Encryption Equipment Worldwide, December 1991, pp. 267-271

[45] *Report to the Nation on Crime and Justice*, U.S. Department of Justice, October 1983

[46] Rivest, R., A. Shamir, and L. Adelman, "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems", *Communications of the ACM*, February 1978, pp. 120-126

[47] Schweitzer, Peter, "Cryptographic Issue Statements Submitted to the Computer System Security and Privacy Advisory Board", NIST spokesman, 27 May 1993, pp. 200-3

[48] Simmons, G., *Contemporary Cryptology*, IEEE Press, 1992

[49] Skrzycki, Cindy, "America Online Slashes Its User Fees", *The Washington Post*, Business Section, 21 April 1993

[50] Solms, Von S., and Naccache, D., "On Blind Signatures and Perfect Crimes", *Computers and Security*, Vol. 11, No. 6, October 1992, pp. 581-3

[51] Spragins, John D., Hammond, Joseph L., and Pavlikowski, Krzysztof, *Telecommunications Protocols and Design*, Addison-Wesley, 1991

[52] "Supercomputer Speed Record - Sandia /Intel Claim 143.4 Double-Presicion GFLOPS", *Technology Forecasts and Technology Surveys*, Vol. 26, No.6, June 1994

[53] "Tap Dance: Keeping Communications Networks Safe for Bugging", *Scientific American*, June 1992

[54] *The Corrections Handbook*, Criminal Justice Institute, 1982

[55] "The National Information Infrastructure: Agenda for Action", Information Infrastructure Task Force, Department of Commerce, 15 September 1993

[56] *Time to Build?*, Edna McConnell Clark Foundation, New York, 1984

[57] Walling, V.C., Jr., Parker, D.B., and Wood, C.C., "Impacts of Federal Policy Options for Nonmilitiary Cryptography", *SRI International Research Report 32*, April 1981

[58] Wayner, Peter, Statement in "Cryptographic Issue Statements Submitted to the Computer System Security and Privacy Advisory Board", National Institute of Standards and Technology, 27 May 1993, pp. 13-17

[59] Wiessman, Clark, "A National Debate on Encryption Exportability", *Communications of the ACM*, Vol. 34, No. 10, 10 October 1991, p. 162

[60] Williams, Peter, "OSISEC Introduction and Overview", University College, London, 15 April 1993

[61] Zimmerman, Philip, Pretty Good Privacy 2.2 Manual, 6 March 1993

APPENDIX A

PROCEDURES FOR IMPLEMENTING DIGITAL TELEPHONY MODEL

Appendix A contains the procedures for the implementing the Digital Telephony Model.

APPENDIX A
PROCEDURES FOR IMPLEMENTING DIGITAL TELEPHONY MODEL

I. Procedures for Installation:

1. Copy the files DigTelModel.wsh and DigTelModel.mac to a Microsoft Excel4.0 directory on a Macintosh (or a PC and convert to Excel DOS).

2. Open the DigTelModel.wsh worksheet and display the two macro buttons.

3. Select a macro button by pressing the Macintosh Command (propeller) key and clicking on the button (in the Macintosh) (reference Microsoft Excel User's Guide 2, Chapter 6, "Automating Tasks with Command Macros").

4. Under the menu select "Macro - Assign To Object..." and redefine the associated macro by selecting "Digital_Telephony_Model" for the "Run Model" button or "Parametric_Tabulation" for the "Calculate and Plot Parametric Values" button.

5. Repeat Steps 3 and 4 for the other command macro button.

6. Open the DigTelModel.mac macros. When associating the button with the macros, Excel sometimes updates the references to the worksheet (DigTelModel.wsh) with part of the path to that file. Unfortunately, the macros will probably not run with the automatic Excel path.

7. Delete path information placed before "DigTelModel.wsh" for any occurrence. (This will occur in 'SET.NAME()' commands (reference Microsoft Excel Function Reference).)

8. With the above steps to redefine the associations between the worksheet and the macros the model should run successfully.

APPENDIX A
PROCEDURES FOR IMPLEMENTING DIGITAL TELEPHONY MODEL (CONT.)

II. Procedures For Running Digital Telephony Cost/ Risks/Benefits Model:

1. Add or delete parameter values as needed for a particular issue. (Note: Parameters listed for other issues, as marked in the "Issue" column do NOT need to be deleted.)

2. Verify that line numbers are consecutive under the "Line Number" column and that the "Selection Criteria" and "Parametric Criteria" were not modified when parameters were added to the database.

3. Add line numbers if the line numbers do not extend to the end of the database and insert the new number of lines in the four occurrences of "400" in the macros.

4. Add values for each required parameter.

5. For each parameter that represents a cost figure, fill-in a 1 in the "Requirements" column , and fill-in the "Issue Number" and "Side of the Issue Number".

6. Fill-in the "Issue Number" and the "Number of Sides to the Issue" in the Command Macro Box at the top, right of the Worksheet.

7. Depress the "Run Model" button, and a table of total costs for each side of the issue will be generated.

III. Procedures For Running Digital Telephony Parametric Model:

1. Follow procedures 1-6 above.

2. For the parameter to be varied, fill-in a 1 in the "Parameter" column, and fill-in the "Starting", "Finishing", and "Step Values" for the parameter.

APPENDIX A
PROCEDURES FOR IMPLEMENTING DIGITAL TELEPHONY MODEL (CONT.)

3. Depress the "Run Parametric Model" button, and a table of total costs for each side of the issue for each value of the parameter will be generated. Following the table generation, a plot of the parametric values vs. total cost for each side of the issue will be generated.

APPENDIX B

DIGITAL TELEPHONY DATABASE

Appendix B contains all database information used for the Digital Telephony Model. It is expandable, as described in Appendix A (Digital Telephony Model Procedures). The database provides the framework for entering all pertinent information and for running the model.

APPENDIX B
DIGITAL TELEPHONY DATABASE

DIGITAL TELEPHONY MODEL								ISSUE 1: Security Equipment Tradeoff		
COST/RISKS/BENEFITS MODEL								ISSUE 2: Implementation of Security Capability		
								ISSUE 3: Implementation of Tap Capability		
								ISSUE 4: Clipper Chip Implementation		
								ISSUE 5: Registration of Keys		
								ISSUE 6: Export Control of Cryptography		
COST ELEMENTS:	**PARAMETERS:**	**METRIC:**	**REQS:**	**ISSUE:**	**SIDE:**	**PARAM:**	**START VALUE:**	**STEP VALUE:**	**END VALUE:**	**NOM VALUE:**
SECURITY IMPLEMENTATION TRADEOFF:										
Cost of First Set of Equipment	Cost of Each Complete Unit	dollars/unit		1	1					200
	Number of Units	integer		1	1					20
	Total Cost of Units	dollars	1	1	1					4,000
	Cost of Installation	dollars	1	1	1					2,500
	Cost of Maintenance/Year	dollars	1	1	1					150
Cost of Second Set of Equipment	Cost of Each Complete Unit	dollars/unit		1	2					50
	Number of Units	integer		1	2					40
	Total Cost of Units	dollars	1	1	2					2,000
	Cost of Installation	dollars	1	1	2					500
	Cost of Maintenance/Year	dollars	1	1	2					10,000
IMPLEMENTATION OF SECURITY CAPABILITY:										
Implementation of Security Capability Apriori	Number of Receivers/Transmitters	integer		2	1					42
	Added Cost per Receiver/Transmitter	dollars/R/T		2	1					35,000
	Total Receiver/Transmitter Cost	dollars	1	2	1					1,470,000
	Added Annual Operations Cost	dollars/year	1	2	1					20,000
	One-time Design/Development Cost	dollars	1	2	1					10,000
Utilization of Security Capability (Apriori)	Key Generation/Distr. (Initial)	dollars	1	2	1					8,400
	Key Generation/Distr. (On-going)	dollars/year	1	2	1					4,200
	Key Management	dollars	1	2	1					8,400
	Key Storage	dollars	1	2	1					2,100
Additional Maintenance	Additional Years Maintained	years		2	1					3
	Additional Cost	dollars	1	2	1					104,100
Depreciation For Initial Installation (Until Delayed Installation)	Depreciation	dollars/year		2	1					73,500
	Total Depreciation	dollars	1	2	1					220,500
Implementation of Security Capability Aposteriori	Number of Receivers/Transmitters	integer		2	2					42
	Percent of Receivers/Transmitters	percent		2	2	1	0.00	0.10	1.00	0.25
	Cost to Modify Each R/T Pair	dollars/R/T		2	2					52,500
	Total Modification Cost for R/T	dollars	1	2	2					551,250
	Annual Added Operations Cost	dollars/year	1	2	2					20,000
	One-time Design/Development Cost	dollars	1	2	2					10,000
Utilization of Security Capability (Aposteriori)	Key Generation/Distr./R/T (Initial)	dollars/R/T		2	2					200
	Total Key Generation/Distr. (Initial)	dollars	1	2	2					2,100
	Key Generation/Distr./R/T (On-going)	dollars/yr/R/T		2	2					100
	Total Key Generation/Distr. (On-going)	dollars	1	2	2					1,050
	Key Management/R/T	dollars/R/T		2	2					200

APPENDIX B
DIGITAL TELEPHONY DATABASE

	Total Key Management	dollars	1	2	2					2,100
	Key Storage/R/T	dollars/R/T		2	2					50
	Total Key Storage	dollars	1	2	2					525
IMPLEMENTATION OF TAP CAPABILITY:										
Implementation of Tap Capability Apriori	Number of Switches in US	integer		3	1					10,000
	Added Cost per Switch	dollars/switch		3	1					25,000
	Total Cost for Switches	dollars		3	1					250,000,000
	Total Cost Amortized Over 5 Yrs-Est.	dollars/5 yrs		3	1					275,000,000
	Total per year	dollars/yr	1	3	1					55,000,000
	One-time Design/Devel. Cost/Vendor	dollars/vendor		3	1					80,000
	Number of Vendors	integer		3	1					6
	Total One-time Design/Devel. Cost	dollars	1	3	1					480,000
Manage & Operate Tap Capability (Apriori)	Added Staff Years/Switch	years		3	1					0
	Average Loaded Labor Hour	dol/yr/switch		3	1					75,000
	Total Operating Cost	dollars	1	3	1					0
Utilization of Tap Capability (Apriori)	Investigation	dollars	1	3	1					0
(Added Cost)	Acquisition of Evidence	dollars	1	3	1					500,000
	Prosecution	dollars	1	3	1					0
	Incarceration	dollars/year	1	3	1					0
Systems Affected By Tap Capability (In General):										
Public Mail Systems	Number of Telephone Company Systems	integer		3	1					6
	Number of Users per Telephone Co.	integer		3	1					1,000,000
	Total Number of Users	integer		3	1					6,000,000
Telephone Switches	No. of Residential Telephone Subscribers	integer		3	1					260,000,000
	Percent Using Digital Switches	percent		3	1					0.90
	No. Res. Subscribers Using Digital Sw.	integer		3	1					26,000,000
	Cost per Digital Switch	dollars/sw		3	1					0
	Total Cost for Switches	dollars		3	1					0
	Number of Business Subscribers	integer		3	1					10,000,000
	Percent with PBX Switches	percent		3	1					0.75
	No. of Bus. Subscribers W/PBX Switches	integer		3	1					7,500,000
	Cost per PBX Switch	dollars/sw		3	1					0
	Total Cost of PBX Switches	dollars		3	1					0
On-line Information Software	Number of Users Effected	integer		3	1					5,000,000
	Cost per User	dollars/user		3	1					0
	Total Cost for Users	dollars		3	1					0
LANs, MANs, and WANs	Number of Networks to be Modified	integer		3	1					1,500,000
	Cost per Network	dollars/net		3	1					0
	Total Cost for Networks	dollars		3	1					0
Radio and Cellular Based Comm Systems	Number of Systems to be Modified	integer		3	1					0
	Cost per System	dollars/system		3	1					0
	Total Cost for Systems	dollars		3	1					0
BBS Systems	Number of Systems to be Modified	integer		3	1					0
	Cost per System	dollars/system		3	1					0
	Total Cost for Systems	dollars		3	1					0
Satellite Uplink/Downlink Equipment	Number of Systems to be Modified	integer		3	1					0
	Cost per System	dollars/system		3	1					0
	Total Cost for Systems	dollars		3	1					0

APPENDIX B
DIGITAL TELEPHONY DATABASE

Aviation Comm Systems	Number of Systems to be Modified	integer		3	1					0
	Cost per System	dollars/system		3	1					0
	Total Cost for Systems	dollars		3	1					0
Implementation of Tap Capability Aposteriori	Number of Switches in US	integer		3	2					10,000
	Percentage of Switches Tapped	percent		3	2	1	0.00	0.01	0.10	0.01
	Number of Switches Tapped	integer		3	2					100
	Cost to Modify Each Switch	dollars/switch		3	2					250,000
	Total Switch Modification Cost	dollars	1	3	2					25,000,000
Manage & Operate Tap Capability (Aposteriori)	Added Staff Years/Switch	years		3	2					0
	Average Loaded Labor Hour	dol/yr/switch		3	2					75,000
	Total Operating Cost	dollars	1	3	2					0
Utilization of Tap Capability (Aposteriori)	Investigation	dollars	1	3	2					0
(Added Cost)	Acquisition of Evidence	dollars	1	3	2					500,000
	Prosecution	dollars	1	3	2					0
	Incarceration	dollars/year	1	3	2					0
CLIPPER CHIP IMPLEMENTATION:										
Effected Equipment	Number of U.S. Phones	integer		4	1					260,000,000
Clipper Chip Device	Cost per Chip (lots of 10000)	dollars/chip		4	1					30
	Percentage of Phones Using Clipper Chip	percent		4	1					0.90
	Total Chip Cost	dollars	1	4	1					7,020,000,000
Installation Costs	One Time Design Integration Cost	dollars	1	4	1					10,000
	Integration Cost per Phone	dollars/phone		4	1					5
	Total Cost for Phone Integration	dollars	1	4	1					1,170,000,000
Wiretap Costs	Number of Wiretap Installations 1990	integer		4	1					872
	Average Cost/Installation (Est. 1990)	dollars/inst.		4	1					45,125
	Total Cost of Wiretaps (Est. 1990)	dollars	1	4	1					39,349,000
REGISTRATION OF KEYS:										
Computing/Storage Facilities	Cost of Equipment (Annual Basis)	dollars/yr	1	5	1					1,500,000
Facility Maintenance	Cost of Maintenance	dollars/yr	1	5	1					120,000
Cost of Registration	Labor Costs	dollars/yr	1	5	1					1,200,000
Overhead	Cost of Facilities	dollars/yr	1	5	1					24,000
	Cost of Management	dollars/yr	1	5	1					170,000
EXPORT CONTROL OF CRYPTOGRAPHY:										
	Target Year	year		6	1		0	1	20	5
	Total Value of Sales (International)	dollars/yr		6	1					33,591,020
	U.S. Market Share	percent		6	1					0.70
	Fraction of U.S. Market Share Prevented	percent		6	1		0.00	0.10	1.00	0.90
	Total Sales Prevented per Year	dollars/yr	1	6	1					21,162,342
RISK ELEMENTS:	**PARAMETERS:**	**METRIC:**	**REQS:**	**ISSUE:**	**SIDE:**	**PARAM:**	**START VALUE:**	**STEP VALUE:**	**END VALUE:**	**NOM VALUE:**
EQUIPMENT TRADEOFF:										
Cost of Security Breakage with Equipment Set #1	Cost of Repairing Damage	dollars	1	1	1					3,000
	Cost of Adding Additional Security	dollars	1	1	1					0

APPENDIX B
DIGITAL TELEPHONY DATABASE

Cost of Security Breakage with Equipment Set #2	Cost of Repairing Damage	dollars	1	1	2					500
	Cost of Adding Additional Security	dollars	1	1	2					0
IMPLEMENTATION OF SECURITY CAPABILITY:										
Compromise of Sensitive Employee Information	Cost of Legal Services	dollars	1	2	2					0
	Cost of Lost Suits	dollars	1	2	2					0
Loss of Trade Secrets/Competitor Advantage	Lost Profits	dollars	1	2	2					200,000
	Cost of Legal Services	dollars	1	2	2					10,000
Sabotage/Loss of Valuable Records	Cost of Losses	dollars	1	2	2					0
IMPLEMENTATION OF TAP CAPABILITY:										
Risks of Designing In Security Taps (Apriori):										
Misuse of Tap Capability (Telco Employees)	Percent of Switches Misused	percent								0.00
	Cost per Misuse	dollars/incident								1,000,000
	Total Cost of Misuse	dollars	1	3	1					10,000,000
Misuse of Info Acquired Legally	Damage/Invasion of Privacy	dollars	1	3	1					0
Compromise of Right to Privacy	Subjective Assessment	dollars	1	3	1					0
Tap Capability Negated or Avoided	Cost of Crimes Avoiding Tap	dollars	1	3	1					1,000,000
Risks of Designing In Security Taps (Aposteriori):										
Misuse of Tap Capability (Telco Employees)	Percent of Switches Misused	percent								0.00
	Cost per Misuse	dollars/incident								1,000,000
	Total Cost of Misuse	dollars	1	3	2					100,000
Misuse of Info Acquired Legally	Damage/Invasion of Privacy	dollars	1	3	2					0
Compromise of Right to Privacy	Subjective Assessment	dollars	1	3	2					0
Tap Capability Negated or Avoided	Cost of Crimes Avoiding Tap	dollars	1	3	2					1,000,000
REGISTRATION OF KEYS:										
Unauthorized Access Resulting In:										
Invasion of Privacy	Probability of Occurance	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					0
	Probable Cost	dollars	1	5	2					0
Bribery	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					2,000,000
	Probable Cost	dollars	1	5	2					-200
Extortion	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					2,000,000
	Probable Cost	dollars	1	5	2					-200
Loss of Trade Secrets	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					10,000,000
	Probable Cost	dollars	1	5	2					-100
Defecation of Character	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					50,000
	Probable Cost	dollars	1	5	2					-0.05
Scandal	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					5,000,000
	Probable Cost	dollars	1	5	2					-50
Insider Trading	Probability of Occurence	percent		5	2					0.00
	Cost of Occurence	dol/occurrence		5	2					7,000,000
	Probable Cost	dollars	1	5	2					-70
EXPORT CONTROL OF CRYPTOGRAPHY:										

APPENDIX B
DIGITAL TELEPHONY DATABASE

Benefit Projection Erased by Foreign Products	Probability of Foreign Products Used	percent		6	1	1	0.00	0.10	1.00	0.50
	Amount of Value Erased	dollars/yr	1	6	1					25,000,000
BENEFIT ELEMENTS:	**PARAMETERS:**	**METRIC:**	**REQS:**	**ISSUE:**	**SIDE:**	**PARAM:**	**START VALUE:**	**STEP VALUE:**	**END VALUE:**	**NOM VALUE:**
EQUIPMENT TRADEOFF:										
Benefits of Using Equipment Set #1	Prevented Value of Lost Information	dollars	1	1	1					0
	Saved Labor Hours	hours								-52
	Average Cost per Labor Hour	dollars/hour								20
	Total Labor Cost Saved	dollars	1	1	1					-1,040
	Prevented Personal Info Leakage Costs	dollars	1	1	1					-2,000
	Saved Legal Fees	dollars	1	1	1					-1,000
Benefits of Using Equipment Set #2	Prevented Value of Lost Information	dollars	1	1	2					0
	Saved Labor Hours	hours		1	2					0
	Average Cost per Labor Hour	dollars/hour		1	2					0
	Total Labor Cost Saved	dollars	1	1	2					0
	Prevented Personal Info Leakage Costs	dollars	1	1	2					-1,000
	Saved Legal Fees	dollars	1	1	2					-500
BENEFITS OF ADDING SECURITY TO COMM SYSTEMS										
Authentication of Information	Value of Correct Information	dollars	1	2	1					-20,000
IMPLEMENTATION OF TAP CAPABILITY (Apriori):										
Courts/Police Costs	Estimated Judicial Expenses 1981	dollars/hr		3	1					100
		hr/day		3	1					8
		days/year		3	1					250
		dollars		3	1					200,000
	Police Costs 1984	dollars/yr		3	1					20,000,000
Prison Costs	Average Cost of Institutional Bed 1982	dollars/yr		3	1					50,000
	Average Cost of Max Security Bed 1982	dollars/yr		3	1					1,000,000
	Number of Corrections Employees 1982	integer		3	1					0
	Cost for Correction Facilities 1982	dollars/yr		3	1					10,000,000,000
Cost of Crimes	Val. of Human Life(Dependants' Support	dollars		3	1					0
	Value of Human Life(Loss of Loved One	dollars		3	1					0
	Value of Recoverable Property	dollars		3	1					0
	Value of Confiscatable Property/Cash	dollars		3	1					0
	Cost to Society	dollars		3	1					0
Cost of Crimes Involving Digital Telephony:										
Bribery	Value of Bribes Paid/Recovered/Fines	dollars		3	1					0
Burglaries	Number Reported in 1983	integer		3	1					5,300,000
	Value of Losses	dollars		3	1					4,000,000,000
Drug Smuggling/Sale	Cost of Addiction Programs (Direct)	dollars		3	1					10,000,000
	Cost of Addiction Programs (Indirect)	dollars		3	1					0
	Recovery/Confiscation Val. of Prop/Cash	dollars		3	1					0
Extortion	Recovery of Value from Extortion	dollars		3	1					0

APPENDIX B
DIGITAL TELEPHONY DATABASE

Insider Trading	Value of Illegal Gains Recovered/Fines	dollars		3	1					0
Murder	Estimated Cost in 1984	dollars		3	1					282,000
	Val. of Human Life(Dependants' Suppor	dollars		3	1					0
	Value of Human Life(Loss of Loved One	dollars		3	1					0
Price Fixing	Cost to Society (Direct)	dollars		3	1					0
	Cost to Society (Indirect)	dollars		3	1					0
Rape	Estimated Cost w/o Bodily Injury 1984	dollars		3	1					24,000
	Estimated Cost w/Bodily Injury in 1984	dollars		3	1					47,000
Robbery	Estimated Cost of Serious Injury 1983	dollars		3	1					32,000
	Cost of Property	dollars		3	1					500,000,000
Scandals (S&L, etc.)	Cost to Corporation	dollars		3	1					-1,000,000
	Cost to Taxpayer	dollars		3	1					-50,000,000,000
Terrorist Activity	Destruction of Property	dollars		3	1					-50,000,000
	Destruction of Life	dollars		3	1					-50,000,000
	Cost of Prevention Agencies (U.S. only)	dollars		3	1					-25,000,000
White Collar Crimes	Number of White Collar Crimes	cases/yr		3	1					500
	Cost per Incident	dollars/case		3	1		-100,000	-100,000	-10,000,000	-100,000
	Total Cost	dollars		3	1					-50,000,000
Crime Totals	Total Criminal Justice Spending	dollars		3	1					-35,000,000,000
	Total Cost of Crime	dollars		3	1					-85,000,000,000
	Rise in Crime Cost	factor		3	1	1	1	1	10	1
	Projected Cost of Crime	dollars		3	1					-85,000,000,000
Amount of Telephony Crime	Percent of Crimes Using Telephony	percent		3	1		0.00	0.01	0.50	0.15
	Cost of Crimes Using Telephony	dollars		3	1					-12,768,900,000
Value of Crime Prevented	Percent of Telephony Crime Deterred	percent		3	1					0.50
	Value of Crime Deterred	dollars	1	3	1					-6,384,450,000
IMPLEMENTATION OF TAP CAPABILITY (Aposteriori):										
Benefit Not Derived Due to Late Implementation	Percent of Crime Not Deterred	percent		3	2					0.02
Crime Prevented	Total Cost of Crime	dollars	1	3	2					-6,256,761,000
CLIPPER CHIP IMPLEMENTATION:										
Wiretap Statistics	Number of Resulting Arrests 1990	Integer		4	2					2,057
	Number of Resulting Arrests from 1989	Integer		4	2					1,486
	Percent of Arrests Leading to Conviction	percent		4	2					0.55
Clipper Chip Benefit	Percent of Targets Using Clipper Chip	percent		4	1	1	0.00	0.10	1.00	0.80
	Number of Convictions Resulting w/CC	Integer		4	2					1,559
	Total Non-Traffic Arrests	Integer		4	2					11,000,000
	Number of Convictions from Wiretaps	Integer		4	2					6,050,000
	Total Cost of Crime	dollars		4	2					28,000,000,000
	Total Cost of Crime Involving Wiretaps	dollars		4	2					15,400,000,000
	Total Cost of Crime Involving CC	dollars	1	4	1					-12,320,000,000
	Value of Crime Prevented per Conviction	dollars/conv.		4	2					2,500
	Total Deterrence Monetary Benefit	dollars	1	4	1					-3,897,300
REGISTRATION OF KEYS:										
Wiretap Statistics	Number of Resulting Arrests 1990	Integer		5	2					2,057
	Number of Resulting Arrests from 1989	Integer		5	2					1,486
	Percent of Arrests Leading to Conviction	percent		5	2					0.55
Key Registration Benefit	% Targets w/Keys Properly Registered	percent		5	2	1	0.00	0.10	1.00	0.50
	Number of Resulting Convictions	Integer		5	2					974

APPENDIX B
DIGITAL TELEPHONY DATABASE

	Total Non-Traffic Arrests	integer		5	2					11,000,000
	Number ofConvictions from Wiretaps	integer		5	2					6,050,000
	Total Cost of Crime	dollars		5	2					28,000,000,000
	Total Cost of Crime Involving Wiretaps	dollars		5	2					15,400,000,000
	Total Cost of Crime Involving Reg. Keys	dollars	1	5	2					7,700,000,000
	Value of Crime Prevented per Conviction	dollars/conv.		5	2					2,500
	Total Deterrence Monetary Benefit	dollars	1	5	2					2,435,813
EXPORT CONTROL OF CRYPTOGRAPHY:										
Crimes Undetectable If U.S. Products Allowed	Value of Crimes Affected	dollars/yr	1	6	1					-50,000,000

APPENDIX C

DIGITAL TELEPHONY DATABASE SELECTION CRITERIA

Appendix C contains the selection criteria used by the Digital Telephony macros to select parameters from the database while tabulating total costs.

APPENDIX C
DIGITAL TELEPHONY DATABASE SELECTION CRITERIA

Digital Telephony Model			Parametric Tabulation								
Issue Number	4		Issue Number	4							
Number Of Sides	1		Side Number	1							
Selection Criteria											
COST ELEMENTS:	PARAMETERS:	METRIC:	REQS:	ISSUE:	SIDE:	PARAM:	START VALUE:	END VALUE:	STEP VALUE:	NOM VALUE:	LINE NUMBER
			1	4	1						81
Parametric Criteria											
COST ELEMENTS:	PARAMETERS:	METRIC:	REQS:	ISSUE:	SIDE:	PARAM:	START VALUE:	END VALUE:	STEP VALUE:	NOM VALUE:	LINE NUMBER
				4	1	1					

APPENDIX D

DIGITAL TELEPHONY MODEL MACROS

Appendix D contains the three macros used to implement the Digital Telephony Model. The first macro, Digital Telephony Model, calculates the total costs for each side of an issue based on the parameter values in the Digital Telephony database. The second macro, Parametric Tabulation, calculates the total costs for the case in which one parameter is varied over a range of values. The third macro, Plot Parametric Values, is called by the Parametric Tabulation macro to plot the Total Cost vs. the Parametric Values.

APPENDIX D
DIGITAL TELEPHONY MODEL MACROS

Variables:	Commands:	Comments:
	Digital_Telephony_Model	Command Function to Compute Total Costs for Each Side of an Issue
	=MESSAGE(TRUE,"INITIALIZING")	Send Status Message to Message Window
SheetName	=SET.NAME("SheetName",GET.WINDOW(1))	Determine the Active Worksheet
TelephonyD	=SET.NAME("TelephonyDbase","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$A$7	Set Pointer to Telephony Database
ModelResult	=SET.NAME("ModelResults","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$M$17)	Set Pointer to Results Area
SelectionCri	=SET.NAME("SelectionCriteria","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$M$7	Set Pointer to Selection Criteria for Parameters
ISSUE_NUME	=SET.NAME("ISSUE_NUMBER",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'	Retrieve the Issue Number
NUM_SIDES	=SET.NAME("NUM_SIDES",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!N	Retrieve the Number of Sides to the Issue to be Used
	=IF(ALERT("ABOUT TO OVERWRITE PREVIOUS MODEL RESULTS",1))	Prompt for User to Continue or Quit
NUM_LINES	=SET.NAME("NUM_LINES",INPUT("Enter the Number of Lines in the Database:",1,,"400"))	Input the Current Number of Lines in the Database
	=FORMULA(1,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$P$8)	Set "REQS:" to 1 in the Selection Criteria
	=FORMULA(ISSUE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$Q$8)	Set "ISSUE:" in the Selection Criteria
	=SELECT(OFFSET(ModelResults,0,0,10,3))	Select Output Area
	=CLEAR(1)	Clear Previous Results
	=SELECT(OFFSET(ModelResults,0,0,1,2))	Select New Header Output Area
	=BORDER(1)	Outline Header Area
	=SELECT(OFFSET(ModelResults,0,1,NUM_SIDES+1,1))	Select New Column Output Area
	=BORDER(1)	Outline Columns
	=SELECT(OFFSET(ModelResults,0,0,NUM_SIDES+1,2))	Select New Results Area
OUTPUT_AF	=SET.NAME("OUTPUT_AREA",SELECTION())	Set Pointer to Results Area
	=BORDER(2)	Outline Results Area
	=ECHO(TRUE)	Turn Off Screen/Window Update to Speed up Macro Execution
TOTAL_COS	=SET.NAME("TOTAL_COST",0)	Initialize Total Cost
SIDE_NUMBE	=SET.NAME("SIDE_NUMBER",1)	Initialize Side Number
	=SELECT(OFFSET(ModelResults,0,0))	Write First Column Header
	=FORMULA("SIDE_NUMBER")	
	=SELECT(OFFSET(ModelResults,0,1))	Write Second Column Header
	=FORMULA("TOTAL_COST")	
	=MESSAGE(TRUE,"GENERATING RESULTS TABLE")	Send Status Message to Message Window
	=FOR("SIDE_NUMBER",1,NUM_OF_SIDES,1)	Output Results for Each Side
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!R8)	Set "SIDE:" in the Selection Criteria
	=FORMULA(SIDE_NUMBER)	
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$X$8)	Clear Line Number in the Selection Criteria
	=FORMULA("")	
	=SELECT(OFFSET(ModelResults,SIDE_NUMBER,0))	Output Side Number to Results Table
	=FORMULA(SIDE_NUMBER)	
NUM_PARAI	=SET.NAME("NUM_PARAMS",DCOUNT(TelephonyDbase,,SelectionCriteria))	Determine the Number of Active Parameters
TOTAL_COS	=SET.NAME("TOTAL_COST",0)	Initialize Total Cost for This Side Number
PARAM_NUI	=SET.NAME("PARAM_NUM",1)	Initialize Parameter Number
CurrentInde	=SET.NAME("CurrentIndex",1)	Initialize Current Index
	=FOR("PARAM_NUM",1,NUM_PARAMS,1)	Tabulate Total Cost for This Side Number
ModelIndex	=SET.NAME("ModelIndex",1)	Initialize Model Index
	=FOR("ModelIndex",CurrentIndex,NUM_LINES,1)	Find Next Parameter
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$X$8)	Write Current Line Number in the Selection Criteria
	=FORMULA(ModelIndex)	
	=IF(ISNUMBER(DGET(TelephonyDbase,"NOM VALUE:",SelectionCriteria)))	Determine if the Current Line Number Contains Added Cost
CurrentInde	=SET.NAME("CurrentIndex",ModelIndex+1)	Save Parameter Index
ModelIndex	=SET.NAME("ModelIndex",NUM_LINES)	Set Model Index to Exit Loop
	=END.IF()	
	=NEXT()	
PARAM_COS	=SET.NAME("PARAM_COST",DGET(TelephonyDbase,"NOM VALUE:",SelectionCriteria))	Retrieve Parameter Cost
TOTAL_COS	=SET.NAME("TOTAL_COST",TOTAL_COST+PARAM_COST)	Total Parameter Cost
	=NEXT()	
	=SELECT(OFFSET(OUTPUT_AREA,SIDE_NUMBER,1))	Write Total Cost to Results Area
	=FORMULA(TOTAL_COST)	
	=NEXT()	
	=END.IF()	
	=RETURN()	

APPENDIX D
DIGITAL TELEPHONY MODEL MACROS

Variables:	Commands:	Comments:
	Parametric_Tabulation	Command Function to Compute Total Costs as a Parameter is Varied
	=MESSAGE(TRUE,"INITIALIZING")	Send Status Message to Message Window
SheetName	=SET.NAME("SheetName",GET.WINDOW(1))	Determine the Active Worksheet
TelephonyD	=SET.NAME("TelephonyDbase","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$A$7	Set Pointer to Telephony Database
ModelResult	=SET.NAME("ModelResults","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$P$17)	Set Pointer to Results Area
SelectionCri	=SET.NAME("SelectionCriteria","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$M$7	Set Pointer to Selection Criteria for Parameters
ParametricC	=SET.NAME("ParametricCriteria","Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!M	Set Pointer to Parametric Criteria for Parameters
ISSUE_NUME	=SET.NAME("ISSUE_NUMBER",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'	Retrieve the Issue Number
SIDE_NUMBE	=SET.NAME("SIDE_NUMBER",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$	Retrieve the Number of Sides to the Issue to be Used
	=IF(ALERT("ABOUT TO OVERWRITE PREVIOUS MODEL RESULTS",1))	Prompt for User to Continue or Quit
	::=IF(FALSE)	Temporary
NUM_LINES	=SET.NAME("NUM_LINES",INPUT("Enter the Number of Lines in the Database:",1,,"400"))	Input the Current Number of Lines in the Database
ISSUE_NUME	=FORMULA(ISSUE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$O$13)	Set "ISSUE:" in the Parametric Criteria
SIDE_NUMBE	=FORMULA(SIDE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$R$13)	Set "SIDE:" in the Parametric Criteria
	=FORMULA(1,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$S$13)	Set "PARAM:" to 1 in the Parametric Criteria
StartValue	=SET.NAME("StartValue",DGET(TelephonyDbase,"START VALUE:",ParametricCriteria))	Retrieve Parametric Starting Value
FinishValue	=SET.NAME("FinishValue",DGET(TelephonyDbase,"END VALUE:",ParametricCriteria))	Retrieve Parametric Ending Value
StepValue	=SET.NAME("StepValue",DGET(TelephonyDbase,"STEP VALUE:",ParametricCriteria))	Retrieve Parametric Step Value
NUM_VALUE	=SET.NAME("NUM_VALUES",((FinishValue-StartValue)/StepValue)+1)	Determine the Number of Parametric Values
Save	=SET.NAME("Save",DGET(TelephonyDbase,"NOM VALUE:",ParametricCriteria))	Save the Parametric Nominal Value
LineNumber	=SET.NAME("LineNumber",DGET(TelephonyDbase,"LINE NUMBER",ParametricCriteria))	Retrieve the Line Number for the Parameter to Vary
	=FORMULA(1,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$P$8)	Set "REQS:" to 1 in the Selection Criteria
	=FORMULA(ISSUE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$Q$8)	Set "ISSUE:" in the Selection Criteria
	=SELECT(OFFSET(ModelResults,0,0,200,4))	Select Output Area
	=CLEAR(1)	Clear Previous Results
	=SELECT(OFFSET(ModelResults,0,0,1,3))	Select New Header Output Area
	=BORDER(1)	Outline Header Area
	=SELECT(OFFSET(ModelResults,0,1,NUM_VALUES+1,1))	Select New Column Output Area
	=BORDER(1)	Outline Columns
	=SELECT(OFFSET(ModelResults,0,0,NUM_VALUES+1,3))	Select New Results Area
OUTPUT_AR	=SET.NAME("OUTPUT_AREA",SELECTION())	Set Pointer to Results Area
	=BORDER(2)	Outline Results Area
	=ECHO(TRUE)	Turn Off Screen/Window Update to Speed up Macro Execution
TOTAL_COS	=SET.NAME("TOTAL_COST",0)	Initialize Total Cost
	=SELECT(OFFSET(ModelResults,0,0))	Write First Column Header
	=FORMULA("SIDE_NUMBER")	
	=SELECT(OFFSET(ModelResults,0,1))	Write Second Column Header
	=FORMULA("PARAM_VALUE")	
	=SELECT(OFFSET(ModelResults,0,2))	Write Third Column Header
	=FORMULA("TOTAL_COST")	
	=SELECT(OFFSET(ModelResults,1,0))	Write First Side Number to Results Area
	=FORMULA(SIDE_NUMBER)	
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$R$8)	Set "SIDE:" in Selection Criteria
	=FORMULA(SIDE_NUMBER)	
	=MESSAGE(TRUE,"GENERATING RESULTS TABLE")	Send Status Message to Message Window
VALUE_NUM	=FOR("VALUE_NUM",1,NUM_VALUES,1)	Output Results for Each Parametric Value
PARAM_VAL	=SET.NAME("PARAM_VALUE",StartValue+((VALUE_NUM-1)*StepValue))	Set "SIDE:" in the Selection Criteria
	=SELECT(OFFSET(TelephonyDbase,LineNumber,10))	Write Current Parameter Value to Database
	=FORMULA(PARAM_VALUE)	
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$X$8)	Clear Line Number in the Selection Criteria
	=FORMULA("")	
NUM_PARAM	=SET.NAME("NUM_PARAMS",DCOUNT(TelephonyDbase,,SelectionCriteria))	Determine the Number of Active Parameters
TOTAL_COS	=SET.NAME("TOTAL_COST",0)	Initialize Total Cost for This Parameter Value
PARAM_NUI	=SET.NAME("PARAM_NUM",1)	Initialize Parameter Number
CurrentInde	=SET.NAME("CurrentIndex",1)	Initialize Current Index
	=FOR("PARAM_NUM",1,NUM_PARAMS,1)	Tabulate Total Cost for This Parameter Value
ModelIndex	=SET.NAME("ModelIndex",1)	Initialize Model Index
	=FOR("ModelIndex",CurrentIndex,NUM_LINES,1)	Find Next Parameter
	=SELECT('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!X8)	Write Current Line Number in the Selection Criteria
	=FORMULA(ModelIndex)	
	=IF(ISNUMBER(DGET(TelephonyDbase,"NOM VALUE:",SelectionCriteria)))	Determine if the Current Line Number Contains Added Cost
CurrentInde	=SET.NAME("CurrentIndex",ModelIndex+1)	Save Parameter Index
ModelIndex	=SET.NAME("ModelIndex",NUM_LINES)	Set Model Index to Exit Loop
	=END.IF()	
	=NEXT()	
PARAM_COS	=SET.NAME("PARAM_COST",DGET(TelephonyDbase,"NOM VALUE:",SelectionCriteria))	Retrieve Parameter Cost
TOTAL_COS	=SET.NAME("TOTAL_COST",TOTAL_COST+PARAM_COST)	Total Parameter Cost
	=NEXT()	
	=SELECT(OFFSET(OUTPUT_AREA,VALUE_NUM,1))	Write Parameter Value to Results Area
	=FORMULA(PARAM_VALUE)	
	=SELECT(OFFSET(OUTPUT_AREA,VALUE_NUM,2))	Write Total Cost to Results Area
	=FORMULA(TOTAL_COST)	
	=NEXT()	

APPENDIX D
DIGITAL TELEPHONY MODEL MACROS

	=SELECT(OFFSET(TelephonyDbase,LineNumber,10))	Write the Nominal Parameter Value Back to the Database
	=FORMULA(Save)	
	=MESSAGE(TRUE,"PLOTTING PARAMETRIC VALUES")	Send Status Message to Message Window
	::=END.IF()	Temporary
	=Plot_Parametric_Values()	Call Parametric Plotting Function
	=END.IF()	
	=RETURN()	

APPENDIX D
DIGITAL TELEPHONY MODEL MACROS

Variables:	Commands:	Comments:
	Plot_Parametric_Values	Macro Function to Plot Parametric Values
SheetName	=SET.NAME("SheetName",GET.WINDOW(1))	Determine the Active Worksheet
ISSUE_NUME	=SET.NAME("ISSUE_NUMBER",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!	Retrieve the Issue Number
SIDE_NUMBE	=SET.NAME("SIDE_NUMBER",DEREF('Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$	Retrieve the Side Number
	=FORMULA(ISSUE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$O$13)	Set "ISSUE:" in Parametric Criteria
	=FORMULA(SIDE_NUMBER,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$R$13)	Set "SIDE:" in Parametric Criteria
	=FORMULA(1,'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!$S$13)	Set "PARAM:" to 1 in Parametric Criteria
	=NEW(2,3,TRUE)	Create a New Chart
Plot	=SET.NAME("Plot",GET.WINDOW(1))	Set Pointer to Active Database
	=SELECT("Chart")	Select Chart
	=CLEAR(3)	Clear Chart
	=GALLERY.SCATTER(2,TRUE)	Set Chart to Connected X-Y Scatter Mode
	=ACTIVATE(SheetName)	Activate the Worksheet
	=ACTIVATE(Plot)	Activate the Plot
X	=SET.NAME("X",'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!R18:R167)	Set Pointer to X-Values
Y	=SET.NAME("Y",'Macintosh HD:DigTel.Bck:FinalVersion:DigTelModel.wsh'!Q18:Q167)	Set Pointer to Y-Values
	=EDIT.SERIES(0,1,Y,X)	Plot X-Y Data Values
	=ATTACH.TEXT(1)	Attach Title to Plot
	=FORMULA(INPUT("Enter Title for Parametric Plot:",2,,"Digital Telephony Parametric Plot"))	
	=SELECT("Title")	Format Title
	=FORMAT.FONT(0,3,TRUE,"Helvitica",14,TRUE,TRUE,FALSE,FALSE,FALSE,FALSE)	
	=ATTACH.TEXT(2)	Attach Y-Axis Label
	=FORMULA(INPUT("Enter Y-Axis Label for Parametric Plot:",2,,"Total Cost"))	
	=ATTACH.TEXT(3)	Attach X-Axis Label
	=FORMULA(INPUT("Enter X-Axis Label for Parametric Plot:",2,,"Parametric Value"))	
	=ECHO(TRUE)	
	=RETURN()	